Códigos electrónicos

Protección de Datos de Carácter Personal

Selección y ordenación:
Santiago Jiménez García, Abogado del Estado.

Edición actualizada a 28 de noviembre de 2018

BOLETÍN OFICIAL DEL ESTADO

La última versión de este Código en PDF y ePUB está disponible para su descarga **gratuita** en:
www.boe.es/legislacion/codigos/

Alertas de actualización en BOE a la Carta: www.boe.es/a_la_carta/

Para adquirir el Código en formato papel: tienda.boe.es

© Agencia Estatal Boletín Oficial del Estado
NIPO (PDF): 007-14-179-0
NIPO (Papel): 007-14-205-4
NIPO (ePUB): 007-14-180-3
ISBN: 978-84-340-2157-0
Depósito Legal: M-33794-2014

Catálogo de Publicaciones de la Administración General del Estado
publicacionesoficiales.boe.es

Agencia Estatal Boletín Oficial del Estado
Avenida de Manoteras, 54
28050 MADRID
tel. 911 114 000 – www.boe.es

SUMARIO

NORMATIVA ESTATAL

§ 1. Constitución Española. [Inclusión parcial] 1

§ 2. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal 2

§ 3. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal 22

§ 4. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones 76

§ 5. Resolución de 22 de junio de 2001, de la Subsecretaría, por la que se dispone la publicación del Acuerdo de Consejo de Ministros por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información 88

§ 6. Orden de 2 de febrero de 1995 por la que se aprueba la primera relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos 90

§ 7. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) 92

§ 8. Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos 182

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

§ 9. Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos 191

§ 10. Resolución de 24 de mayo de 2010, de la Agencia Española de Protección de Datos, por la que se regula el Registro Electrónico de la Agencia Española de Protección de Datos 203

§ 11. Resolución de 18 de marzo de 2010, de la Agencia Española de Protección de Datos, por la que se crea la Sede Electrónica de la Agencia Española de Protección de Datos 208

§ 12. Resolución de 1 de septiembre de 2006, de la Agencia Española de Protección de Datos, por la que se determina la información que contiene el Catálogo de ficheros inscritos en el Registro General de Protección de Datos 211

§ 13. Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se crea el Registro Telemático de la Agencia Española de Protección de Datos 214

§ 14. Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de 218

inscripción de ficheros en el Registro General de Protección de Datos, así como los formatos y requerimientos a los que deben ajustarse las notificaciones remitidas en soporte informático o telemático . . . . .

§ 15. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras 224

§ 16. Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones 229

§ 17. Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos 232

§ 18. Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo . . 239

§ 19. Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación 241

§ 20. Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios 245

§ 21. Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal . . 247

§ 22. Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito 249

NORMATIVA AUTONÓMICA

§ 23. Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos 252

§ 24. Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos 265

NORMATIVA ESTATAL SECTORIAL

§ 25. Ley 7/2017, de 2 de noviembre, por la que se incorpora al ordenamiento jurídico español la Directiva 2013/11/UE, del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo. [Inclusión parcial] 278

§ 26. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. [Inclusión parcial] 280

§ 27. Acuerdo de 23 de julio de 2015, del Pleno del Tribunal Constitucional, por el que se regula la exclusión de los datos de identidad personal en la publicación de las resoluciones jurisdiccionales . 284

§ 28. Ley 23/2015, de 21 de julio, Ordenadora del Sistema de Inspección de Trabajo y Seguridad Social. [Inclusión parcial] 286

§ 29. Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado. [Inclusión parcial] 290

§ 30. Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito. [Inclusión parcial] 292

Sumario

§ 31. Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. [Inclusión parcial] 297

§ 32. Ley 5/2014, de 4 de abril, de Seguridad Privada. [Inclusión parcial] 303

§ 33. Ley 26/2013, de 27 de diciembre, de cajas de ahorros y fundaciones bancarias. [Inclusión parcial] . 311

§ 34. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. [Inclusión parcial] 313

§ 35. Ley Orgánica 3/2013, de 20 de junio, de protección de la salud del deportista y lucha contra el dopaje en la actividad deportiva. [Inclusión parcial] 317

§ 36. Ley 4/2013, de 4 de junio, de medidas de flexibilización y fomento del mercado del alquiler de viviendas. [Inclusión parcial] 322

§ 37. Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia. [Inclusión parcial] 324

§ 38. Ley 33/2011, de 4 de octubre, General de Salud Pública. [Inclusión parcial] 326

§ 39. Ley 29/2011, de 22 de septiembre, de Reconocimiento y Protección Integral a las Víctimas del Terrorismo. [Inclusión parcial] 328

§ 40. Ley 26/2011, de 1 de agosto, de adaptación normativa a la Convención Internacional sobre los Derechos de las Personas con Discapacidad. [Inclusión parcial] 329

§ 41. Ley 23/2011, de 29 de julio, de depósito legal. [Inclusión parcial] 330

§ 42. Ley Orgánica 9/2011, de 27 de julio, de derechos y deberes de los miembros de las Fuerzas Armadas. [Inclusión parcial] 332

§ 43. Ley 20/2011, de 21 de julio, del Registro Civil. [Inclusión parcial] 334

§ 44. Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia. [Inclusión parcial] 336

§ 45. Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación. [Inclusión parcial] 343

§ 46. Ley 13/2011, de 27 de mayo, de regulación del juego. [Inclusión parcial] 346

§ 47. Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal. [Inclusión parcial] 351

§ 48. Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. [Inclusión parcial] 353

§ 49. Ley Orgánica 2/2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo. [Inclusión parcial] 361

§ 50. Ley 54/2007, de 28 de diciembre, de Adopción internacional. [Inclusión parcial] 363

§ 51. Ley Orgánica 11/2007, de 22 de octubre, reguladora de los derechos y deberes de los miembros de la Guardia Civil. [Inclusión parcial] 364

§ 52. Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN. [Inclusión parcial] 365

§ 53. Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades 366

Sumario

§ 54. Ley Orgánica 2/2006, de 3 de mayo, de Educación. [Inclusión parcial] 400

§ 55. Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género. [Inclusión parcial] 402

§ 56. Ley 59/2003, de 19 de diciembre, de firma electrónica. [Inclusión parcial] 403

§ 57. Ley 58/2003, de 17 de diciembre, General Tributaria. [Inclusión parcial] 406

§ 58. Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas. [Inclusión parcial] 411

§ 59. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica 413

§ 60. Ley Orgánica 1/2002, de 22 de marzo, reguladora del Derecho de Asociación. [Inclusión parcial] . . 425

§ 61. Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. [Inclusión parcial] 427

§ 62. Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social. [Inclusión parcial] 429

§ 63. Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. [Inclusión parcial] 432

§ 64. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. [Inclusión parcial] 435

ÍNDICE SISTEMÁTICO

NORMATIVA ESTATAL

§ 1. Constitución Española. [Inclusión parcial] 1

[. . .]

TÍTULO I. De los derechos y deberes fundamentales 1
CAPÍTULO SEGUNDO. Derechos y libertades 1
Sección 1.ª De los derechos fundamentales y de las libertades públicas 1

§ 2. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal 2

Preámbulo 2
TÍTULO I. Disposiciones generales 2
TÍTULO II. Principios de la protección de datos 4
TÍTULO III. Derechos de las personas 7
TÍTULO IV. Disposiciones sectoriales 9
CAPÍTULO I. Ficheros de titularidad pública 9
CAPÍTULO II. Ficheros de titularidad privada 11
TÍTULO V. Movimiento internacional de datos 14
TÍTULO VI. Agencia de Protección de Datos 15
TÍTULO VII. Infracciones y sanciones 18
Disposiciones adicionales 18
Disposiciones transitorias 20
Disposiciones derogatorias 20
Disposiciones finales 20

§ 3. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal 22

Preámbulo 22
Artículos 24
Disposiciones transitorias 24
Disposiciones derogatorias 25
Disposiciones finales 26
REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL 26
TÍTULO I. Disposiciones generales 26
TÍTULO II. Principios de protección de datos 30
CAPÍTULO I. Calidad de los datos 30
CAPÍTULO II. Consentimiento para el tratamiento de los datos y deber de información 32
Sección 1.ª Obtención del consentimiento del afectado 32
Sección 2.ª Deber de información al interesado 34
CAPÍTULO III. Encargado del tratamiento 34
TÍTULO III. Derechos de acceso, rectificación, cancelación y oposición 36
CAPÍTULO I. Disposiciones generales 36
CAPÍTULO II. Derecho de acceso 37
CAPÍTULO III. Derechos de rectificación y cancelación 39
CAPÍTULO IV. Derecho de oposición 40
TÍTULO IV. Disposiciones aplicables a determinados ficheros de titularidad privada 41
CAPÍTULO I. Ficheros de información sobre solvencia patrimonial y crédito 41

Sección 1.ª Disposiciones generales . . . 41
Sección 2.ª Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés . . . 41
CAPÍTULO II. Tratamientos para actividades de publicidad y prospección comercial . . . 44
TÍTULO V. Obligaciones previas al tratamiento de los datos. . . . 46
CAPÍTULO I. Creación, modificación o supresión de ficheros de titularidad pública . . . 46
CAPÍTULO II. Notificación e inscripción de los ficheros de titularidad pública o privada . . . 47
TÍTULO VI. Transferencias internacionales de datos . . . 50
CAPÍTULO I. Disposiciones generales . . . 50
CAPÍTULO II. Transferencias a estados que proporcionen un nivel adecuado de protección . . . 50
CAPÍTULO III. Transferencias a Estados que no proporcionen un nivel adecuado de protección . . . 51
TÍTULO VII. Códigos tipo. . . . 52
TÍTULO VIII. De las medidas de seguridad en el tratamiento de datos de carácter personal . . . 55
CAPÍTULO I. Disposiciones generales . . . 55
CAPÍTULO II. Del documento de seguridad . . . 57
CAPÍTULO III. Medidas de seguridad aplicables a ficheros y tratamientos automatizados . . . 59
Sección 1.ª Medidas de seguridad de nivel básico . . . 59
Sección 2.ª Medidas de seguridad de nivel medio. . . . 60
Sección 3.ª Medidas de seguridad de nivel alto . . . 62
CAPÍTULO IV. Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados . . . 63
Sección 1.ª Medidas de seguridad de nivel básico . . . 63
Sección 2.ª Medidas de seguridad de nivel medio. . . . 63
Sección 3.ª Medidas de seguridad de nivel alto . . . 64
TÍTULO IX. Procedimientos tramitados por la Agencia Española de Protección de Datos . . . 64
CAPÍTULO I. Disposiciones generales . . . 64
CAPÍTULO II. Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición . . . 65
CAPÍTULO III. Procedimientos relativos al ejercicio de la potestad sancionadora . . . 66
Sección 1.ª Disposiciones generales . . . 66
Sección 2.ª Actuaciones previas . . . 66
Sección 3.ª Procedimiento sancionador . . . 68
Sección 4.ª Procedimiento de declaración de infracción de la Ley Orgánica 15/1999, de 13 de diciembre, por las administraciones públicas . . . 68
CAPÍTULO IV. Procedimientos relacionados con la inscripción o cancelación de ficheros . . . 68
Sección 1.ª Procedimiento de inscripción de la creación, modificación o supresión de ficheros . . . 68
Sección 2.ª Procedimiento de cancelación de oficio de ficheros inscritos . . . 69
CAPÍTULO V. Procedimientos relacionados con las transferencias internacionales de datos . . . 70
Sección 1.ª Procedimiento de autorización de transferencias internacionales de datos . . . 70
Sección 2.ª Procedimiento de suspensión temporal de transferencias internacionales de datos . . . 71
CAPÍTULO VI. Procedimiento de inscripción de códigos tipo . . . 72
CAPÍTULO VII. Otros procedimientos tramitados por la agencia española de protección de datos . . . 73
Sección 1.ª Procedimiento de exención del deber de información al interesado . . . 73
Sección 2.ª Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos . . . 74
Disposiciones adicionales . . . 74
Disposiciones finales . . . 75

§ 4. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones . . . 76

Preámbulo . . . 76
CAPÍTULO I. Disposiciones generales . . . 78
CAPÍTULO II. Conservación y cesión de datos . . . 80
CAPÍTULO III. Infracciones y sanciones . . . 82
Disposiciones adicionales . . . 82
Disposiciones transitorias . . . 84
Disposiciones derogatorias . . . 84
Disposiciones finales . . . 84

§ 5. Resolución de 22 de junio de 2001, de la Subsecretaría, por la que se dispone la publicación del Acuerdo de Consejo de Ministros por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información . . . 88

Preámbulo . . . 88
ANEXO. Acuerdo por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información . . . 88

§ 6. Orden de 2 de febrero de 1995 por la que se aprueba la primera relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos . . . 90

Preámbulo . . . 90
Artículos . . . 90
Disposiciones finales . . . 91

§ 7. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) . . . 92

Preámbulo . . . 92
CAPÍTULO I. Disposiciones generales . . . 127
CAPÍTULO II. Principios . . . 131
CAPÍTULO III. Derechos del interesado . . . 135
Sección 1. Transparencia y modalidades . . . 135
Sección 2. Información y acceso a los datos personales . . . 136
Sección 3. Rectificación y supresión . . . 138
Sección 4. Derecho de oposición y decisiones individuales automatizadas . . . 140
Sección 5. Limitaciones . . . 141
CAPÍTULO IV. Responsable del tratamiento y encargado del tratamiento . . . 142
Sección 1. Obligaciones generales . . . 142
Sección 2. Seguridad de los datos personales . . . 146
Sección 3. Evaluación de impacto relativa a la protección de datos y consulta previa . . . 147
Sección 4. Delegado de protección de datos . . . 149
Sección 5. Códigos de conducta y certificación . . . 151
CAPÍTULO V. Transferencias de datos personales a terceros países u organizaciones internacionales . . . 155
CAPÍTULO VI. Autoridades de control independientes . . . 160
Sección 1. Independencia . . . 160
Sección 2. Competencia, funciones y poderes . . . 161
CAPÍTULO VII. Cooperación y coherencia . . . 165
Sección 1. Cooperación y coherencia . . . 165
Sección 2. Coherencia . . . 168
Sección 3. Comité europeo de protección de datos . . . 170
CAPÍTULO VIII. Recursos, responsabilidad y sanciones . . . 174
CAPÍTULO IX. Disposiciones relativas a situaciones específicas de tratamiento . . . 177
CAPÍTULO X. Actos delegados y actos de ejecución . . . 179
CAPÍTULO XI. Disposiciones finales . . . 180

§ 8. Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos . . . 182

Preámbulo . . . 182
CAPÍTULO I. Inspección en materia de protección de datos . . . 185
CAPÍTULO II. Régimen sancionador en materia de protección de datos . . . 185
CAPÍTULO III. Procedimientos en caso de posible vulneración de la normativa de protección de datos . . . 186
Disposiciones adicionales . . . 189
Disposiciones transitorias . . . 190
Disposiciones derogatorias . . . 190
Disposiciones finales . . . 190

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

§ 9. Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos . . . 191

Preámbulo . . . 191
Artículos . . . 191
Disposiciones adicionales . . . 191
Disposiciones finales . . . 191

ESTATUTO DE LA AGENCIA DE PROTECCIÓN DE DATOS . . . 192
Capítulo I. Disposiciones generales . . . 192
Capítulo II. Funciones de la Agencia de Protección de Datos . . . 192
Capítulo III. Organos de la Agencia de Protección de Datos . . . 194
Sección 1. Estructura orgánica de la Agencia de Protección de Datos . . . 194
Sección 2. El Director de la Agencia de Protección de Datos . . . 194
Sección 3. El Consejo Consultivo . . . 196
Sección 4. El Registro General de Protección de Datos . . . 198
Sección 5. La Inspección de Datos . . . 199
Sección 6. La Secretaría General . . . 200
CAPITULO IV. Régimen económico, patrimonial y de personal . . . 200
Sección 1. Régimen económico . . . 200
Sección 2. Régimen patrimonial . . . 201
Sección 3. Régimen del personal . . . 201
Disposiciones adicionales . . . 202

§ 10. Resolución de 24 de mayo de 2010, de la Agencia Española de Protección de Datos, por la que se regula el Registro Electrónico de la Agencia Española de Protección de Datos . . . 203

Preámbulo . . . 203
Artículos . . . 204
Disposiciones transitorias . . . 207
Disposiciones derogatorias . . . 207
Disposiciones finales . . . 207
ANEXO I. Procedimientos competencia de la Agencia Española de Protección de Datos admisibles a través de su Registro Electrónico . . . 207

§ 11. Resolución de 18 de marzo de 2010, de la Agencia Española de Protección de Datos, por la que se crea la Sede Electrónica de la Agencia Española de Protección de Datos . . . 208

Preámbulo . . . 208
Artículos . . . 209
Disposiciones finales . . . 210

§ 12. Resolución de 1 de septiembre de 2006, de la Agencia Española de Protección de Datos, por la que se determina la información que contiene el Catálogo de ficheros inscritos en el Registro General de Protección de Datos . . . 211

Preámbulo . . . 211
Artículos . . . 212

§ 13. Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se crea el Registro Telemático de la Agencia Española de Protección de Datos . . . 214

Preámbulo . . . 214
Artículos . . . 215

§ 14. Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos, así como los formatos y requerimientos a los que deben ajustarse las notificaciones remitidas en soporte informático o telemático . . . 218

Preámbulo . . . 218
Artículos . . . 221
ANEXOS . . . 223

§ 15. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras . . . 224

Preámbulo . . . 224
Artículos . . . 226
Disposiciones transitorias . . . 227

Disposiciones finales . . . 227
ANEXO. 1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. . . . 227

§ 16. Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones . . . 229

Preámbulo . . . 229
Artículos . . . 230

§ 17. Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos . . . 232

Preámbulo . . . 232
Sección I. Disposiciones generales . . . 234
Sección II. Disposiciones aplicables a transferencias concretas . . . 235

§ 18. Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo . . . 239

Preámbulo . . . 239
Artículos . . . 239

§ 19. Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación . . . 241

Preámbulo . . . 241
Artículos . . . 241
Disposiciones finales . . . 244

§ 20. Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios . . . 245

Preámbulo . . . 245
Artículos . . . 245

§ 21. Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal . . . 247

Preámbulo . . . 247
Artículos . . . 247

§ 22. Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito . . . 249

Preámbulo . . . 249
CAPÍTULO I. Calidad de los datos objeto del tratamiento automatizado, forma y veces en que debe efectuarse la notificación y cómputo del plazo al que se refiere el artículo 28.3 de la Ley Orgánica . . . 250
CAPITULO II. Medidas de seguridad . . . 251

NORMATIVA AUTONÓMICA

§ 23. Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos . . . 252

Preámbulo . . . 252

TÍTULO I. Disposiciones generales . . . 254
TÍTULO II. La Agencia Vasca de Protección de Datos . . . 257
TÍTULO III. Régimen sancionador . . . 261
Disposiciones adicionales . . . 263
Disposiciones finales . . . 264

§ 24. Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos . . . 265

Preámbulo . . . 265
CAPÍTULO I. Disposiciones generales . . . 266
CAPÍTULO II. Organización . . . 268
CAPÍTULO III. Relaciones con otros organismos e instituciones . . . 271
CAPÍTULO IV. Ejercicio de competencias y funciones . . . 272
CAPÍTULO V. Régimen jurídico, de personal, económico y de contratación . . . 275
Disposiciones transitorias . . . 276
Disposiciones derogatorias . . . 277
Disposiciones finales . . . 277

NORMATIVA ESTATAL SECTORIAL

§ 25. Ley 7/2017, de 2 de noviembre, por la que se incorpora al ordenamiento jurídico español la Directiva 2013/11/UE, del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo. [Inclusión parcial] . . . 278

[. . .]

TÍTULO II. Obligaciones de las entidades de resolución alternativa acreditadas . . . 278

§ 26. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. [Inclusión parcial] . . . 280

TÍTULO PRELIMINAR. Disposiciones generales, principios de actuación y funcionamiento del sector público . . . 280
CAPÍTULO I. Disposiciones generales . . . 280
CAPÍTULO V. Funcionamiento electrónico del sector público . . . 281

[. . .]

§ 27. Acuerdo de 23 de julio de 2015, del Pleno del Tribunal Constitucional, por el que se regula la exclusión de los datos de identidad personal en la publicación de las resoluciones jurisdiccionales . . . 284

Preámbulo . . . 284
Artículos . . . 284
Disposiciones transitorias . . . 284
Disposiciones finales . . . 285

§ 28. Ley 23/2015, de 21 de julio, Ordenadora del Sistema de Inspección de Trabajo y Seguridad Social. [Inclusión parcial] . . . 286

[. . .]

TÍTULO II. Funcionamiento del Sistema . . . 286
CAPÍTULO I. De las funciones de la Inspección de Trabajo y Seguridad Social . . . 286
CAPÍTULO II. De las actuaciones de la Inspección de Trabajo y Seguridad Social . . . 288

[. . .]

§ 29. Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado. [Inclusión parcial] . . . 290

[. . .]

TÍTULO III. Órganos de vigilancia y control de los altos cargos de la Administración General del Estado . . . 290

§ 30. Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito. [Inclusión parcial] 292

TÍTULO I. De las entidades de crédito 292
CAPÍTULO I. Disposiciones generales 292

[. . .]

TÍTULO III. Supervisión. 294
CAPÍTULO I. Función supervisora 294
CAPÍTULO VI. Obligaciones de información y publicación 295

§ 31. Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. [Inclusión parcial] 297

[. . .]

TÍTULO III. Obligaciones de servicio público y derechos y obligaciones de carácter público en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas 297

[. . .]

CAPÍTULO III. Secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas 297

[. . .]

§ 32. Ley 5/2014, de 4 de abril, de Seguridad Privada. [Inclusión parcial] 303

[. . .]

TÍTULO I. Coordinación 303
TÍTULO IV. Servicios y medidas de seguridad 303

[. . .]

CAPÍTULO II. Servicios de las empresas de seguridad privada 304
CAPÍTULO III. Servicios de los despachos de detectives privados 304
TÍTULO VI. Régimen sancionador 306
CAPÍTULO I. Infracciones 306

§ 33. Ley 26/2013, de 27 de diciembre, de cajas de ahorros y fundaciones bancarias. [Inclusión parcial] 311

TÍTULO II. De las fundaciones bancarias 311

[. . .]

CAPÍTULO V. Régimen de control 311

§ 34. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. [Inclusión parcial] 313

[. . .]

TÍTULO I. Transparencia de la actividad pública 313

[. . .]

CAPÍTULO II. Publicidad activa 313
CAPÍTULO III. Derecho de acceso a la información pública 314

[. . .]

TÍTULO III. Consejo de Transparencia y Buen Gobierno 315

§ 35. Ley Orgánica 3/2013, de 20 de junio, de protección de la salud del deportista y lucha contra el dopaje en la actividad deportiva. [Inclusión parcial] 317

[. . .]

TÍTULO II. De la salud y del dopaje de los deportistas con licencia deportiva 317
CAPÍTULO I. El dopaje en el ámbito del deporte con licencia deportiva 317
CAPÍTULO III. Protección de la salud 319

[. . .]

CAPÍTULO IV. Del tratamiento de datos relativos al dopaje 319
TÍTULO III. Políticas públicas de control y supervisión general de los productos que pueden utilizarse para el dopaje en la actividad deportiva 320

[. . .]

CAPÍTULO II. De las condiciones de utilización de los productos susceptibles de producir dopaje en la actividad deportiva 320

§ 36. Ley 4/2013, de 4 de junio, de medidas de flexibilización y fomento del mercado del alquiler de viviendas. [Inclusión parcial]. 322

Disposiciones adicionales 323

§ 37. Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia. [Inclusión parcial] 324

[. . .]

CAPÍTULO II. Funciones 324

§ 38. Ley 33/2011, de 4 de octubre, General de Salud Pública. [Inclusión parcial] 326

[. . .]

TÍTULO I. Derechos, deberes y obligaciones en salud pública 326
CAPÍTULO I. Derechos de los ciudadanos 326

[. . .]

CAPÍTULO IX. Sistema de Información en Salud Pública. 326

§ 39. Ley 29/2011, de 22 de septiembre, de Reconocimiento y Protección Integral a las Víctimas del Terrorismo. [Inclusión parcial] 328

[. . .]

TÍTULO CUARTO. Régimen de protección social 328

[. . .]

§ 40. Ley 26/2011, de 1 de agosto, de adaptación normativa a la Convención Internacional sobre los Derechos de las Personas con Discapacidad. [Inclusión parcial] 329

§ 41. Ley 23/2011, de 29 de julio, de depósito legal. [Inclusión parcial] 330

CAPÍTULO I. Disposiciones generales 330
CAPÍTULO II. De la obligación del depósito legal 331

[. . .]

§ 42. Ley Orgánica 9/2011, de 27 de julio, de derechos y deberes de los miembros de las Fuerzas Armadas. [Inclusión parcial] . . . 332

[. . .]

TÍTULO I. Del ejercicio de los derechos fundamentales y libertades públicas . . . 332

§ 43. Ley 20/2011, de 21 de julio, del Registro Civil. [Inclusión parcial] . . . 334

TÍTULO I. El Registro Civil. Disposiciones generales . . . 334
CAPÍTULO PRIMERO. Naturaleza, contenido y competencias del Registro Civil . . . 334

§ 44. Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia. [Inclusión parcial] . . . 336

[. . .]

TÍTULO II. Uso de los medios electrónicos en la Administración de Justicia . . . 336
CAPÍTULO I. Derechos de los ciudadanos en sus relaciones con la Administración de Justicia por medios electrónicos . . . 336
CAPÍTULO II. Derechos y deberes de los profesionales de la justicia en sus relaciones con la Administración de Justicia por medios electrónicos . . . 337
CAPÍTULO III. Utilización obligatoria de los medios electrónicos en la tramitación de los procedimientos electrónicos judiciales . . . 338
TÍTULO III. Régimen jurídico de la Administración judicial electrónica . . . 338
CAPÍTULO I. De la sede judicial electrónica . . . 338
TÍTULO IV. De la tramitación electrónica de los procedimientos judiciales . . . 339

[. . .]

CAPÍTULO II. Del expediente judicial electrónico . . . 339
CAPÍTULO III. Del registro de escritos, las comunicaciones y las notificaciones electrónicas . . . 340

[. . .]

Sección 2.ª De las comunicaciones y las notificaciones electrónicas . . . 341
CAPÍTULO IV. De la tramitación electrónica . . . 341
TÍTULO V. Cooperación entre las Administraciones con competencias en materia de Administración de Justicia. El Esquema judicial de interoperabilidad y seguridad . . . 342
CAPÍTULO I. Marco institucional de cooperación en materia de administración electrónica . . . 342
Disposiciones adicionales . . . 342

§ 45. Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación. [Inclusión parcial] . . . 343

[. . .]

TÍTULO II. Recursos humanos dedicados a la investigación . . . 343
CAPÍTULO I. Personal Investigador al servicio de las Universidades públicas, de los Organismos Públicos de Investigación y de los Organismos de investigación de otras Administraciones Públicas . . . 343

[. . .]

CAPÍTULO II. Especificidades aplicables al personal al servicio de los Organismos Públicos de Investigación de la Administración General del Estado . . . 344

[. . .]

Sección 2.ª Personal de investigación al servicio de los organismos públicos de Investigación de la Administración General del Estado . . . 344

§ 46. Ley 13/2011, de 27 de mayo, de regulación del juego. [Inclusión parcial] . . . 346

[. . .]

TÍTULO IV. Control de la actividad . . . 346

[. . .]

CAPÍTULO II. Participantes . . . 346
CAPÍTULO III. Homologación de los sistemas técnicos de juego . . . 347
TÍTULO V. La Administración del Juego . . . 348

[. . .]

§ 47. Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal. [Inclusión parcial]. . . . 351

[. . .]

TÍTULO II. Derechos de los usuarios de los servicios postales . . . 351
TÍTULO V. Acceso a la red postal de los operadores y resolución de conflictos entre ellos . . . 351
CAPÍTULO I. Acceso a la red postal y a otras infraestructuras postales. . . . 351

[. . .]

§ 48. Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. [Inclusión parcial] . . . 353

[. . .]

CAPÍTULO II. De la diligencia debida . . . 353

[. . .]

Sección 3.ª Medidas reforzadas de diligencia debida. . . . 353
CAPÍTULO III. De las obligaciones de información . . . 354
CAPÍTULO IV. Del control interno. . . . 355

[. . .]

CAPÍTULO VI. Otras disposiciones. . . . 357

[. . .]

§ 49. Ley Orgánica 2/2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo. [Inclusión parcial] . . . 361

[. . .]

TÍTULO II. De la interrupción voluntaria del embarazo . . . 361

[. . .]

CAPÍTULO II. Garantías en el acceso a la prestación . . . 361

§ 50. Ley 54/2007, de 28 de diciembre, de Adopción internacional. [Inclusión parcial] . . . 363

TÍTULO I. Disposiciones generales . . . 363

[. . .]

CAPÍTULO III. Capacidad y requisitos para la adopción internacional . . . 363

[. . .]

§ 51. Ley Orgánica 11/2007, de 22 de octubre, reguladora de los derechos y deberes de los miembros de la Guardia Civil. [Inclusión parcial]. . . . 364

[. . .]

TÍTULO II. Del ejercicio de derechos fundamentales y libertades públicas. . . . 364

§ 52. Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN. [Inclusión parcial] 365

§ 53. Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades 366

Preámbulo 366
Artículos 368
Disposiciones adicionales 391
Disposiciones transitorias 397
Disposiciones finales 397

§ 54. Ley Orgánica 2/2006, de 3 de mayo, de Educación. [Inclusión parcial] 400

[. . .]

§ 55. Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género. [Inclusión parcial]. 402

[. . .]

TÍTULO V. Tutela Judicial 402

[. . .]

CAPÍTULO IV. Medidas judiciales de protección y de seguridad de las víctimas 402

§ 56. Ley 59/2003, de 19 de diciembre, de firma electrónica. [Inclusión parcial]. 403

[. . .]

TÍTULO III. Prestación de servicios de certificación 403
CAPÍTULO I. Obligaciones 403
TÍTULO VI. Infracciones y sanciones 404

§ 57. Ley 58/2003, de 17 de diciembre, General Tributaria. [Inclusión parcial] 406

[. . .]

TÍTULO III. La aplicación de los tributos 406
CAPÍTULO I. Principios generales 406

[. . .]

Sección 3.ª Colaboración social en la aplicación de los tributos 406

[. . .]

§ 58. Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas. [Inclusión parcial] 411

[. . .]

TÍTULO V. Gestión patrimonial 411

[. . .]

CAPÍTULO V. Enajenación y gravamen 411

[. . .]

Sección 2.ª Enajenación de inmuebles 411

§ 59. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica 413

Preámbulo 413
CAPÍTULO I. Principios generales 415
CAPÍTULO II. El derecho de información sanitaria 416
CAPÍTULO III. Derecho a la intimidad 417
CAPÍTULO IV. El respeto de la autonomía del paciente 417
CAPÍTULO V. La historia clínica 420
CAPÍTULO VI. Informe de alta y otra documentación clínica 423
Disposiciones adicionales 423
Disposiciones transitorias 424
Disposiciones derogatorias 424
Disposiciones finales 424

§ 60. Ley Orgánica 1/2002, de 22 de marzo, reguladora del Derecho de Asociación. [Inclusión parcial] 425

[. . .]

CAPÍTULO III. Funcionamiento de las asociaciones 425
CAPÍTULO V. Registros de Asociaciones 425

§ 61. Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. [Inclusión parcial] 427

[. . .]

TÍTULO VII. De la ejecución de las medidas 427

[. . .]

CAPÍTULO II. Reglas para la ejecución de las medidas 427

§ 62. Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social. [Inclusión parcial] 429

[. . .]

TÍTULO II. Régimen jurídico de los extranjeros 429
CAPÍTULO I. De la entrada y salida del territorio español 429

[. . .]

§ 63. Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. [Inclusión parcial] 432

Disposiciones adicionales 433

§ 64. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. [Inclusión parcial] 435

[. . .]

TÍTULO III. De las actuaciones judiciales 435
CAPÍTULO I. De la oralidad, publicidad y lengua oficial 435

[. . .]

LIBRO VIII. Del Consejo General del Poder Judicial 436
TÍTULO I. De las atribuciones del Consejo General del Poder Judicial 436

§ 1

Constitución Española. [Inclusión parcial]

Cortes Generales
«BOE» núm. 311, de 29 de diciembre de 1978
Última modificación: 27 de septiembre de 2011
Referencia: BOE-A-1978-31229

[. . .]

TÍTULO I

De los derechos y deberes fundamentales

[. . .]

CAPÍTULO SEGUNDO

Derechos y libertades

[. . .]

Sección 1.ª De los derechos fundamentales y de las libertades públicas

[. . .]

Artículo 18.

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

[. . .]

§ 2

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

Jefatura del Estado
«BOE» núm. 298, de 14 de diciembre de 1999
Última modificación: 30 de julio de 2018
Referencia: BOE-A-1999-23750

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Artículo 2. *Ámbito de aplicación.*

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.

d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Artículo 3. *Definiciones.*

A los efectos de la presente Ley Orgánica se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de

su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

TÍTULO II

Principios de la protección de datos

Artículo 4. *Calidad de los datos.*

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. *Derecho de información en la recogida de datos.*

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6. *Consentimiento del afectado.*

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 7. *Datos especialmente protegidos.*

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8. *Datos relativos a la salud.*

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Artículo 9. *Seguridad de los datos.*

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. *Deber de secreto.*

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. *Comunicación de datos.*

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.

En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 12. *Acceso a los datos por cuenta de terceros.*

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

TÍTULO III

Derechos de las personas

Artículo 13. *Impugnación de valoraciones.*

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 14. *Derecho de consulta al Registro General de Protección de Datos.*

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. *Derecho de acceso.*

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Artículo 16. *Derecho de rectificación y cancelación.*

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.

Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Artículo 17. *Procedimiento de oposición, acceso, rectificación o cancelación.*

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.

2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Artículo 18. *Tutela de los derechos.*

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia

de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Artículo 19. *Derecho a indemnización.*

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.

3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

TÍTULO IV

Disposiciones sectoriales

CAPÍTULO I

Ficheros de titularidad pública

Artículo 20. *Creación, modificación o supresión.*

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Artículo 21. *Comunicación de datos entre Administraciones públicas.*

1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo **cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o** cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

Téngase en cuenta que se declara la inconstitucionalidad y nulidad del inciso destacado del apartado 1 por Sentencia del TC 292/2000, de 30 de noviembre. Ref. BOE-T-2001-332

2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.

3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

Artículo 22. *Ficheros de las Fuerzas y Cuerpos de Seguridad.*

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. *Excepciones a los derechos de acceso, rectificación y cancelación.*

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. *Otras excepciones a los derechos de los afectados.*

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado **impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas** o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales **o administrativas**.

> Téngase en cuenta que se declara la inconstitucionalidad y nulidad de los incisos destacados del apartado 1 por Sentencia del TC 292/2000, de 30 de noviembre. Ref. BOE-T-2001-332

2. **(Anulado)**

CAPÍTULO II

Ficheros de titularidad privada

Artículo 25. *Creación.*

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. *Notificación e inscripción registral.*

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Artículo 27. *Comunicación de la cesión de datos.*

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

Artículo 28. *Datos incluidos en las fuentes de acceso público.*

1. Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3, j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.

2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial.

Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.

La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique.

En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.

Artículo 29. *Prestación de servicios de información sobre solvencia patrimonial y crédito.*

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

Artículo 30. *Tratamientos con fines de publicidad y de prospección comercial.*

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se

dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.

4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 31. *Censo promocional.*

1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.

2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.

3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento.

Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.

4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.

Artículo 32. *Códigos tipo.*

1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TÍTULO V

Movimiento internacional de datos

Artículo 33. *Norma general.*

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. *Excepciones.*

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público.

Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

TÍTULO VI

Agencia de Protección de Datos

Artículo 35. *Naturaleza y régimen jurídico.*

1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.

2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.

3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.

4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.

b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

c) Cualesquiera otros que legalmente puedan serle atribuidos.

5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 36. *El Director.*

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.

2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas.

En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

Artículo 37. *Funciones.*

1. Son funciones de la Agencia de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.

d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

2. Las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos.

Reglamentariamente podrán establecerse los términos en que se lleve a cabo la publicidad de las citadas resoluciones.

Lo establecido en los párrafos anteriores no será aplicable a las resoluciones referentes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos ni a aquéllas por las que se resuelva la inscripción en el mismo de los Códigos tipo, regulados por el artículo 32 de esta ley orgánica.

Artículo 38. *Consejo Consultivo.*

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

Un Diputado, propuesto por el Congreso de los Diputados.

Un Senador, propuesto por el Senado.

Un representante de la Administración Central, designado por el Gobierno.

Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.

Un miembro de la Real Academia de la Historia, propuesto por la misma.

Un experto en la materia, propuesto por el Consejo Superior de Universidades.

Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.

Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.

Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. *El Registro General de Protección de Datos.*

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros de que sean titulares las Administraciones públicas.

b) Los ficheros de titularidad privada.

c) Las autorizaciones a que se refiere la presente Ley.

d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.

e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 40. *Potestad de inspección.*

(Derogado).

Artículo 41. *Órganos correspondientes de las Comunidades Autónomas.*

1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.

2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.

3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 42. *Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.*

1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento.

2. Si la Administración pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TÍTULO VII

Infracciones y sanciones

Artículo 43. *Responsables.*

(Derogado).

Artículo 44. *Tipos de infracciones.*

(Derogado).

Artículo 45. *Tipo de sanciones.*

(Derogado).

Artículo 46. *Infracciones de las Administraciones públicas.*

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

3. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 47. *Prescripción.*

(Derogado).

Artículo 48. *Procedimiento sancionador.*

(Derogado).

Artículo 49. *Potestad de inmovilización de ficheros.*

(Derogado).

Disposición adicional primera. *Ficheros preexistentes.*

Los ficheros y tratamientos automatizados inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor.

En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Disposición adicional segunda. *Ficheros y Registro de Población de las Administraciones públicas.*

1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.

2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones públicas.

Disposición adicional tercera. *Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social.*

Los expedientes específicamente instruidos al amparo de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido cincuenta años desde la fecha de aquéllos.

En este último supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, pondrá a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos en el párrafo anterior, mediante la utilización de los procedimientos técnicos pertinentes en cada caso.

Disposición adicional cuarta. *Modificación del artículo 112.4 de la Ley General Tributaria.*

El apartado cuarto del artículo 112 de la Ley General Tributaria pasa a tener la siguiente redacción:

"4. La cesión de aquellos datos de carácter personal, objeto de tratamiento, que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado.

En este ámbito tampoco será de aplicación lo que respecto a las Administraciones públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal."

Disposición adicional quinta. *Competencias del Defensor del Pueblo y órganos autonómicos semejantes.*

Lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas.

Disposición adicional sexta. *Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.*

Se modifica el artículo 24.3, párrafo 2.º de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados, con la siguiente redacción:

"Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora.

La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la ley.

También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.

En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado."

Disposición transitoria primera. *Tratamientos creados por Convenios internacionales.*

La Agencia de Protección de Datos será el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio.

Disposición transitoria segunda. *Utilización del censo promocional.*

Reglamentariamente se desarrollarán los procedimientos de formación del censo promocional, de oposición a aparecer en el mismo, de puesta a disposición de sus solicitantes, y de control de las listas difundidas.

El Reglamento establecerá los plazos para la puesta en operación del censo promocional.

Disposición transitoria tercera. *Subsistencia de normas preexistentes.*

Hasta tanto se lleven a efectos las previsiones de la disposición final primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo; 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley.

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal.

Disposición final primera. *Habilitación para el desarrollo reglamentario.*

El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley.

Disposición final segunda. *Preceptos con carácter de Ley ordinaria.*

Los Títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la disposición adicional cuarta, la disposición transitoria primera y la final primera tienen el carácter de Ley ordinaria.

Disposición final tercera. *Entrada en vigor.*

La presente Ley entrará en vigor en el plazo de un mes, contado desde su publicación en el "Boletín Oficial del Estado".

Información relacionada

- Téngase en cuenta que las referencias a la Agencia de Protección de Datos deben entenderse hechas a la Agencia Española de Protección de Datos, según establece el art. 79 de la Ley 62/2003, de 30 de diciembre. Ref. BOE-A-2003-23936

§ 3

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

Ministerio de Justicia
«BOE» núm. 17, de 19 de enero de 2008
Última modificación: 8 de marzo de 2012
Referencia: BOE-A-2008-979

La actual Ley Orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal adaptó nuestro ordenamiento a lo dispuesto por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, derogando a su vez la hasta entonces vigente Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos de carácter personal.

La nueva ley, que ha nacido con una amplia vocación de generalidad, prevé en su artículo 1 que «tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal». Comprende por tanto el tratamiento automatizado y el no automatizado de los datos de carácter personal.

A fin de garantizar la necesaria seguridad jurídica en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos, el legislador declaró subsistentes las normas reglamentarias existentes y, en especial, los reales decretos 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del tratamiento automatizado de los datos de carácter personal y 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, a la vez que habilitó al Gobierno para la aprobación o modificación de las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la Ley Orgánica 15/1999.

Por otra parte, la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones atribuyen competencias en materia sancionadora a la Agencia Española de Protección de Datos. Éstas requieren de desarrollo reglamentario con la peculiaridad de que ambas normas se ordenan a la tutela no sólo de los derechos de las personas físicas, sino también de las jurídicas.

II

Este Reglamento comparte con la Ley Orgánica la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales. Por ello, ha de destacarse que esta norma reglamentaria nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la Ley Orgánica de acuerdo con los principios que emanan de la Directiva, sino también aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo.

Por tanto, se aprueba este Reglamento partiendo de la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema.

III

El reglamento viene a abarcar el ámbito tutelado anteriormente por los reales decretos 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, teniendo en cuenta la necesidad de fijar criterios aplicables a los ficheros y tratamientos de datos personales no automatizados. Por otra parte, la atribución de funciones a la Agencia Española de Protección de Datos por la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones obliga a desarrollar también los procedimientos para el ejercicio de la potestad sancionadora por la Agencia.

El reglamento se estructura en nueve títulos cuyo contenido desarrolla los aspectos esenciales en esta materia.

El título I contempla el objeto y ámbito de aplicación del reglamento. A lo largo de la vigencia de la Ley Orgánica 15/1999, se ha advertido la conveniencia de desarrollar el apartado 2 de su artículo 2 para aclarar qué se entiende por ficheros y tratamientos relacionados con actividades personales o domésticas, aspecto muy relevante dado que están excluidos de la normativa sobre protección de datos de carácter personal.

Por otra parte, el presente reglamento no contiene previsiones para los tratamientos de datos personales a los que se refiere el apartado 3 del artículo 2 de la ley orgánica, dado que se rigen por sus disposiciones específicas y por lo especialmente previsto, en su caso, por la propia Ley Orgánica 15/1999. En consecuencia, se mantiene el régimen jurídico propio de estos tratamientos y ficheros.

Además, en este título se aporta un conjunto de definiciones que ayudan al correcto entendimiento de la norma, lo que resulta particularmente necesario en un ámbito tan tecnificado como el de la protección de datos personales. Por otra parte, fija el criterio a seguir en materia de cómputo de plazos con el fin de homogeneizar esta cuestión evitando distinciones que suponen diferencias de trato de los ficheros públicos respecto de los privados.

El título II, se refiere a los principios de la protección de datos. Reviste particular importancia la regulación del modo de captación del consentimiento atendiendo a aspectos muy específicos como el caso de los servicios de comunicaciones electrónicas y, muy particularmente, la captación de datos de los menores. Asimismo, se ofrece lo que no puede definirse sino como un estatuto del encargado del tratamiento, que sin duda contribuirá a clarificar todo lo relacionado con esta figura. Las previsiones en este ámbito se completan con lo dispuesto en el título VIII en materia de seguridad dotando de un marco coherente a la actuación del encargado.

El título III se ocupa de una cuestión tan esencial como los derechos de las personas en este ámbito. Estos derechos de acceso, rectificación, cancelación y oposición al tratamiento, según ha afirmado el Tribunal Constitucional en su sentencia número 292/2000, constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y «sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer».

A continuación, los títulos IV a VII permiten clarificar aspectos importantes para el tráfico ordinario, como la aplicación de criterios específicos a determinado tipo de ficheros de titularidad privada que por su trascendencia lo requerían -los relativos a la solvencia patrimonial y crédito y los utilizados en actividades de publicidad y prospección comercial-, el conjunto de obligaciones materiales y formales que deben conducir a los responsables a la creación e inscripción de los ficheros, los criterios y procedimientos para la realización de las transferencias internacionales de datos, y, finalmente, la regulación de un instrumento, el código tipo, llamado a jugar cada vez un papel más relevante como elemento dinamizador del derecho fundamental a la protección de datos.

El título VIII regula un aspecto esencial para la tutela del derecho fundamental a la protección de datos, la seguridad, que repercute sobre múltiples aspectos organizativos, de gestión y aún de inversión, en todas las organizaciones que traten datos personales. La repercusión del deber de seguridad obligaba a un particular rigor ya que en esta materia han confluido distintos elementos muy relevantes. Por una parte, la experiencia dimanante de la aplicación del Real Decreto 994/1999 permitía conocer las dificultades que habían enfrentado los responsables e identificar los puntos débiles y fuertes de la regulación. Por otra, se reclamaba la adaptación de la regulación en distintos aspectos. En este sentido, el reglamento trata de ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponda adoptar en cada caso y en la revisión de las mismas cuando ello resulte necesario. Por otra parte, ordena con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad. Además, se ha pretendido regular la materia de modo que contemple las múltiples formas de organización material y personal de la seguridad que se dan en la práctica. Por último, se regula un conjunto de medidas destinadas a los ficheros y tratamientos estructurados y no automatizados que ofrezca a los responsables un marco claro de actuación.

Finalmente en el título IX, dedicado a los procedimientos tramitados por la Agencia Española de Protección de Datos, se ha optado por normar exclusivamente aquellas especialidades que diferencian a los distintos procedimientos tramitados por la Agencia de las normas generales previstas para los procedimientos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya aplicación se declara supletoria al presente reglamento.

En su virtud, a propuesta del Ministro de Justicia, con la aprobación previa de la Ministra de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 21 de diciembre de 2007.

D I S P O N G O :

Artículo único. *Aprobación del reglamento.*

Se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, cuyo texto se incluye a continuación.

Disposición transitoria primera. *Adaptación de los códigos tipo inscritos en el Registro General de Protección de Datos.*

En el plazo de un año desde la entrada en vigor del presente real decreto deberán notificarse a la Agencia Española de Protección de Datos las modificaciones que resulten necesarias en los códigos tipo inscritos en el Registro General de Protección de Datos para adaptar su contenido a lo dispuesto en el título VII del mismo.

Disposición transitoria segunda. *Plazos de implantación de las medidas de seguridad.*

La implantación de las medidas de seguridad previstas en el presente real decreto deberá producirse con arreglo a las siguientes reglas:

1.ª Respecto de los ficheros automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) En el plazo de un año desde su entrada en vigor, deberán implantarse las medidas de seguridad de nivel medio exigibles a los siguientes ficheros:

1.º Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.

2.º Aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

3.º Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, respecto de las medidas de este nivel que no fueran exigibles conforme a lo previsto en el artículo 4.4 del Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio.

b) En el plazo de un año desde su entrada en vigor deberán implantarse las medidas de seguridad de nivel medio y en el de dieciocho meses desde aquella fecha, las de nivel alto exigibles a los siguientes ficheros:

1.º Aquéllos que contengan datos derivados de actos de violencia de género.

2.º Aquéllos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización.

c) En los demás supuestos, cuando el presente reglamento exija la implantación de una medida adicional, no prevista en el Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, dicha medida deberá implantarse en el plazo de un año desde la entrada en vigor del presente real decreto.

2.ª Respecto de los ficheros no automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) Las medidas de seguridad de nivel básico deberán implantarse en el plazo de un año desde su entrada en vigor.

b) Las medidas de seguridad de nivel medio deberán implantarse en el plazo de dieciocho meses desde su entrada en vigor.

c) Las medidas de seguridad de nivel alto deberán implantarse en el plazo de dos años desde su entrada en vigor.

3.ª Los ficheros, tanto automatizados como no automatizados, creados con posterioridad a la fecha de entrada en vigor del presente real decreto deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en el mismo.

Disposición transitoria tercera. *Régimen transitorio de las solicitudes para el ejercicio de los derechos de las personas.*

A las solicitudes para el ejercicio de los derechos de acceso, oposición, rectificación y cancelación que hayan sido efectuadas antes de la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

Disposición transitoria cuarta. *Régimen transitorio de los procedimientos.*

A los procedimientos ya iniciados antes de la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

Disposición transitoria quinta. *Régimen transitorio de las actuaciones previas.*

A las actuaciones previas iniciadas con anterioridad a la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

El presente real decreto se aplicará a las actuaciones previas que se inicien después de su entrada en vigor.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogados el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del

tratamiento automatizado de los datos de carácter personal, el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal y todas las normas de igual o inferior rango que contradigan o se opongan a lo dispuesto en el presente real decreto.

Disposición final primera. *Título competencial.*

El título I, con excepción del apartado c) del artículo 4, los títulos II, III, VII y VIII, así como los artículos 52, 53.3, 53.4, 54, 55.1, 55.3, 56, 57, 58 y 63.3 del reglamento se dictan al amparo de lo dispuesto en el artículo 149.1.1.ª de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor a los tres meses de su íntegra publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente reglamento tiene por objeto el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.

2. Asimismo, el capítulo III del título IX de este reglamento desarrolla las disposiciones relativas al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora, en aplicación de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, en el título VII de la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en el título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 2. *Ámbito objetivo de aplicación.*

1. El presente reglamento será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.

4. Este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

Artículo 3. *Ámbito territorial de aplicación.*

1. Se regirá por el presente reglamento todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español.

Cuando no resulte de aplicación lo dispuesto en el párrafo anterior, pero exista un encargado del tratamiento ubicado en España, serán de aplicación al mismo las normas contenidas en el título VIII del presente reglamento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española, según las normas de Derecho internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

En este supuesto, el responsable del tratamiento deberá designar un representante establecido en territorio español.

2. A los efectos previstos en los apartados anteriores, se entenderá por establecimiento, con independencia de su forma jurídica, cualquier instalación estable que permita el ejercicio efectivo y real de una actividad.

Artículo 4. *Ficheros o tratamientos excluidos.*

El régimen de protección de los datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos:

a) A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.

b) A los sometidos a la normativa sobre protección de materias clasificadas.

c) A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Artículo 5. *Definiciones.*

1. A los efectos previstos en este reglamento, se entenderá por:

a) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.

b) Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

c) Cesión o comunicación de datos: Tratamiento de datos que supone su revelación a una persona distinta del interesado.

d) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

e) Dato disociado: aquél que no permite la identificación de un afectado o interesado.

f) Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

g) Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

h) Destinatario o cesionario: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

i) Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

j) Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

k) Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

l) Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

m) Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

n) Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

ñ) Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

o) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

p) Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.

q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

r) Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

s) Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien

constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

t) Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

2. En particular, en relación con lo dispuesto en el título VIII de este reglamento se entenderá por:

a) Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

b) Autenticación: procedimiento de comprobación de la identidad de un usuario.

c) Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

d) Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

e) Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

f) Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

g) Ficheros temporales: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

h) Identificación: procedimiento de reconocimiento de la identidad de un usuario.

i) Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

j) Perfil de usuario: accesos autorizados a un grupo de usuarios.

k) Recurso: cualquier parte componente de un sistema de información.

l) Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

m) Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

n) Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

ñ) Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

o) Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

p) Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

Artículo 6. *Cómputo de plazos.*

En los supuestos en que este reglamento señale un plazo por días se computarán únicamente los hábiles. Cuando el plazo sea por meses, se computarán de fecha a fecha.

Artículo 7. *Fuentes accesibles al público.*

1. A efectos del artículo 3, párrafo j) de la Ley Orgánica 15/1999, se entenderá que sólo tendrán el carácter de fuentes accesibles al público:

a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.

c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.

d) Los diarios y boletines oficiales.

e) Los medios de comunicación social.

2. En todo caso, para que los supuestos enumerados en el apartado anterior puedan ser considerados fuentes accesibles al público, será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación.

TÍTULO II

Principios de protección de datos

CAPÍTULO I

Calidad de los datos

Artículo 8. *Principios relativos a la calidad de los datos.*

1. Los datos de carácter personal deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

2. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.

3. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4. Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

5. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.

Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.

Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento.

6. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

7. Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

Artículo 9. *Tratamiento con fines estadísticos, históricos o científicos.*

1. No se considerará incompatible, a los efectos previstos en el apartado 3 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos.

Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

2. Por vía de excepción a lo dispuesto en el apartado 6 del artículo anterior, la Agencia Española de Protección de Datos o, en su caso, las autoridades de control de las comunidades autónomas podrán, previa solicitud del responsable del tratamiento y conforme al procedimiento establecido en la sección segunda del capítulo VII del título IX del presente reglamento, acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas a las que se refiere el apartado anterior.

Artículo 10. *Supuestos que legitiman el tratamiento o cesión de los datos.*

1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.

2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:

a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

b) **(Anulado)**

3. Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando:

a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.

b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:

a) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

b) La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.

c) La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos:

Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.

Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.

La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

5. Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.

En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

Artículo 11. *Verificación de datos en solicitudes formuladas a las Administraciones públicas.*

(Anulado)

CAPÍTULO II

Consentimiento para el tratamiento de los datos y deber de información

Sección 1.ª Obtención del consentimiento del afectado

Artículo 12. *Principios generales.*

1. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

2. Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.

3. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

Artículo 13. *Consentimiento para el tratamiento de datos de menores de edad.*

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos.

No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Artículo 14. *Forma de recabar el consentimiento.*

1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.

2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

3. En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

4. Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

5. Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

Artículo 15. *Solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma.*

Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.

En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

Artículo 16. *Tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas.*

La solicitud del consentimiento para el tratamiento o cesión de los datos de tráfico, facturación y localización por parte de los sujetos obligados, o en su caso la revocación de aquél, según la legislación reguladora de las telecomunicaciones se someterá a lo establecido en su normativa específica y, en lo que no resulte contrario a la misma, a lo establecido en la presente sección.

Artículo 17. *Revocación del consentimiento.*

1. El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

2. El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a la solicitud.

4. Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el plazo previsto en el apartado 2, para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre.

Sección 2.ª Deber de información al interesado

Artículo 18. *Acreditación del cumplimiento del deber de información.*

(Anulado)

Artículo 19. *Supuestos especiales.*

En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Encargado del tratamiento

Artículo 20. *Relaciones entre el responsable y el encargado del tratamiento.*

1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo

deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Artículo 21. *Posibilidad de subcontratación de los servicios.*

1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.

Artículo 22. *Conservación de los datos por el encargado del tratamiento.*

1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

TÍTULO III

Derechos de acceso, rectificación, cancelación y oposición

CAPÍTULO I

Disposiciones generales

Artículo 23. *Carácter personalísimo.*

1. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado.

2. Tales derechos se ejercitarán:

a) Por el afectado, acreditando su identidad, del modo previsto en el artículo siguiente.

b) Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.

c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél.

Cuando el responsable del fichero sea un órgano de las Administraciones públicas o de la Administración de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.

3. Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél.

Artículo 24. *Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.*

1. Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

2. Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

4. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.

5. El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aún cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre

que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente.

Artículo 25. *Procedimiento.*

1. Salvo en el supuesto referido en el párrafo 4 del artículo anterior, el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá:

a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.

b) Petición en que se concreta la solicitud.

c) Dirección a efectos de notificaciones, fecha y firma del solicitante.

d) Documentos acreditativos de la petición que formula, en su caso.

2. El responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros.

3. En el caso de que la solicitud no reúna los requisitos especificados en el apartado primero, el responsable del fichero deberá solicitar la subsanación de los mismos.

4. La respuesta deberá ser conforme con los requisitos previstos para cada caso en el presente título.

5. Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta al que se refiere el apartado 2, debiendo conservar la acreditación del cumplimiento del mencionado deber.

6. El responsable del fichero deberá adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

7. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición podrá modularse por razones de seguridad pública en los casos y con el alcance previsto en las Leyes.

8. Cuando las leyes aplicables a determinados ficheros concretos establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos, se estará a lo dispuesto en aquéllas.

Artículo 26. *Ejercicio de los derechos ante un encargado del tratamiento.*

Cuando los afectados ejercitasen sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición.

CAPÍTULO II

Derecho de acceso

Artículo 27. *Derecho de acceso.*

1. El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

2. En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento.

No obstante, cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos.

3. El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 28. *Ejercicio del derecho de acceso.*

1. Al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:

a) Visualización en pantalla.
b) Escrito, copia o fotocopia remitida por correo, certificado o no.
c) Telecopia.
d) Correo electrónico u otros sistemas de comunicaciones electrónicas.
e) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

2. Los sistemas de consulta del fichero previstos en el apartado anterior podrán restringirse en función de la configuración o implantación material del fichero o de la naturaleza del tratamiento, siempre que el que se ofrezca al afectado sea gratuito y asegure la comunicación escrita si éste así lo exige.

3. El responsable del fichero deberá cumplir al facilitar el acceso lo establecido en el Título VIII de este Reglamento.

Si tal responsable ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, aquél no responderá por los posibles riesgos que para la seguridad de la información pudieran derivarse de la elección.

Del mismo modo, si el responsable ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, serán de cuenta del afectado los gastos derivados de su elección.

Artículo 29. *Otorgamiento del acceso.*

1. El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

2. Si la solicitud fuera estimada y el responsable no acompañase a su comunicación la información a la que se refiere el artículo 27.1, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.

3. La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

Artículo 30. *Denegación del acceso.*

1. El responsable del fichero o tratamiento podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.

2. Podrá también denegarse el acceso en los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Derechos de rectificación y cancelación

Artículo 31. *Derechos de rectificación y cancelación.*

1. El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

2. El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento.

En los supuestos en que el interesado invoque el ejercicio del derecho de cancelación para revocar el consentimiento previamente prestado, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente reglamento.

Artículo 32. *Ejercicio de los derechos de rectificación y cancelación.*

1. La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.

2. El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal del afectado deberá igualmente comunicárselo en el mismo plazo.

3. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar o cancelar los datos.

La rectificación o cancelación efectuada por el cesionario no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 33. *Denegación de los derechos de rectificación y cancelación.*

1. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

2. Podrá también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación

directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO IV

Derecho de oposición

Artículo 34. *Derecho de oposición.*

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación.

c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento.

Artículo 35. *Ejercicio del derecho de oposición.*

1. El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento.

Cuando la oposición se realice con base en la letra a) del artículo anterior, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

2. El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

3. El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado 2 de este artículo.

Artículo 36. *Derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos.*

1. Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

TÍTULO IV

Disposiciones aplicables a determinados ficheros de titularidad privada

CAPÍTULO I

Ficheros de información sobre solvencia patrimonial y crédito

Sección 1.ª Disposiciones generales

Artículo 37. *Régimen aplicable.*

1. El tratamiento de datos de carácter personal sobre solvencia patrimonial y crédito, previsto en el apartado 1 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, se someterá a lo establecido, con carácter general, en dicha ley orgánica y en el presente reglamento.

2. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición en el caso de los ficheros a que se refiere el apartado anterior, se rige por lo dispuesto en los capítulos I a IV del título III del presente reglamento, con los siguientes criterios:

a) Cuando la petición de ejercicio de los derechos se dirigiera al responsable del fichero, éste estará obligado a satisfacer, en cualquier caso, dichos derechos.

b) Si la petición se dirigiera a las personas y entidades a las que se presta el servicio, éstas únicamente deberán comunicar al afectado aquellos datos relativos al mismo que les hayan sido comunicados y a facilitar la identidad del responsable para que, en su caso, puedan ejercitar sus derechos ante el mismo.

3. De conformidad con el apartado 2 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, también podrán tratarse los datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés.

Estos datos deberán conservarse en ficheros creados con la exclusiva finalidad de facilitar información crediticia del afectado y su tratamiento se regirá por lo dispuesto en el presente reglamento y, en particular, por las previsiones contenidas en la sección segunda de este capítulo.

Sección 2.ª Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés

Artículo 38. *Requisitos para la inclusión de los datos.*

1. Sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, siempre que concurran los siguientes requisitos:

a) Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada **y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero.**

Téngase en cuenta que se anula el inciso destacado de la letra a) del apartado 1 por Sentencias del TS de 15 de julio de 2010. Ref. BOE-A-2010-16299 y Ref. BOE-A-2010-16301

b) Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

c) Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.

2. **(Anulado)**

3. El acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento de los requisitos establecidos en este artículo y del requerimiento previo al que se refiere el artículo siguiente.

Artículo 39. *Información previa a la inclusión.*

El acreedor deberá informar al deudor, en el momento en que se celebre el contrato y, en todo caso, al tiempo de efectuar el requerimiento al que se refiere la letra c) del apartado 1 del artículo anterior, que en caso de no producirse el pago en el término previsto para ello y cumplirse los requisitos previstos en el citado artículo, los datos relativos al impago podrán ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

Artículo 40. *Notificación de inclusión.*

1. El responsable del fichero común deberá notificar a los interesados respecto de los que hayan registrado datos de carácter personal, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos, informándole asimismo de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, en los términos establecidos por la Ley Orgánica 15/1999, de 13 de diciembre.

2. Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.

3. La notificación deberá efectuarse a través de un medio fiable, auditable e independiente de la entidad notificante, que la permita acreditar la efectiva realización de los envíos.

4. En todo caso, será necesario que el responsable del fichero pueda conocer si la notificación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

No se entenderán suficientes para que no se pueda proceder al tratamiento de los datos referidos a un interesado las devoluciones en las que el destinatario haya rehusado recibir el envío.

5. Si la notificación de inclusión fuera devuelta, el responsable del fichero común comprobará con la entidad acreedora que la dirección utilizada para efectuar esta notificación se corresponde con la contractualmente pactada con el cliente a efectos de comunicaciones y no procederá al tratamiento de los datos si la mencionada entidad no confirma la exactitud de este dato.

Artículo 41. *Conservación de los datos.*

1. Sólo podrán ser objeto de tratamiento los datos que respondan con veracidad a la situación de la deuda en cada momento concreto.

El pago o cumplimiento de la deuda determinará la cancelación inmediata de todo dato relativo a la misma.

2. En los restantes supuestos, los datos deberán ser cancelados cuando se hubieran cumplido seis años contados a partir del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

Artículo 42. *Acceso a la información contenida en el fichero.*

1. Los datos contenidos en el fichero común sólo podrán ser consultados por terceros cuando precisen enjuiciar la solvencia económica del afectado. En particular, se considerará que concurre dicha circunstancia en los siguientes supuestos:

a) Que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida.
b) Que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio.
c) Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

2. Los terceros deberán informar por escrito a las personas en las que concurran los supuestos contemplados en las letras b) y c) precedentes de su derecho a consultar el fichero.
En los supuestos de contratación telefónica de los productos o servicios a los que se refiere el párrafo anterior, la información podrá realizarse de forma no escrita, correspondiendo al tercero la prueba del cumplimiento del deber de informar.

Artículo 43. *Responsabilidad.*

1. El acreedor o quien actúe por su cuenta o interés deberá asegurarse que concurren todos los requisitos exigidos en los artículos 38 y 39 en el momento de notificar los datos adversos al responsable del fichero común.
2. El acreedor o quien actúe por su cuenta o interés será responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 44. *Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.*

1. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición se rige por lo dispuesto en los capítulos I a IV del título III de este reglamento, sin perjuicio de lo señalado en el presente artículo.
2. Cuando el interesado ejercite su derecho de acceso en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirigiera al titular del fichero común, éste deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero.
En este caso, el titular del fichero común deberá, además de dar cumplimiento a lo establecido en el presente reglamento, facilitar las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.
2.ª Si la solicitud se dirigiera a cualquier otra entidad participante en el sistema, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad y dirección del titular del fichero común para que pueda completar el ejercicio de su derecho de acceso.

3. Cuando el interesado ejercite sus derechos de rectificación o cancelación en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirige al titular del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de siete días, procederá a la rectificación o cancelación cautelar de los mismos.
2.ª Si la solicitud se dirige a quien haya facilitado los datos al fichero común procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al titular del fichero

común en el plazo de diez días, dando asimismo respuesta al interesado en los términos previstos en el artículo 33 de este reglamento.

3.ª Si la solicitud se dirige a otra entidad participante en el sistema, que no hubiera facilitado al fichero común los datos, dicha entidad informará al afectado sobre este hecho en el plazo máximo de diez días, proporcionándole, además, la identidad y dirección del titular del fichero común para, que en su caso, puedan ejercitar sus derechos ante el mismo.

CAPÍTULO II

Tratamientos para actividades de publicidad y prospección comercial

Artículo 45. *Datos susceptibles de tratamiento e información al interesado.*

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, así como quienes realicen estas actividades con el fin de comercializar sus propios productos o servicios o los de terceros, sólo podrán utilizar nombres y direcciones u otros datos de carácter personal cuando los mismos se encuentren en uno de los siguientes casos:

a) Figuren en alguna de las fuentes accesibles al público a las que se refiere la letra j) del artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre y el artículo 7 de este reglamento y el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento para las actividades descritas en este apartado.

b) Hayan sido facilitados por los propios interesados u obtenidos con su consentimiento para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, habiéndose informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad.

2. Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, deberá informarse al interesado en cada comunicación que se le dirija del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.

A tal efecto, el interesado deberá ser informado de que sus datos han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos.

Artículo 46. *Tratamiento de datos en campañas publicitarias.*

1. Para que una entidad pueda realizar por sí misma una actividad publicitaria de sus productos o servicios entre sus clientes será preciso que el tratamiento se ampare en alguno de los supuestos contemplados en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre.

2. En caso de que una entidad contrate o encomiende a terceros la realización de una determinada campaña publicitaria de sus productos o servicios, encomendándole el tratamiento de determinados datos, se aplicarán las siguientes normas:

a) Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por la entidad que contrate la campaña, ésta será responsable del tratamiento de los datos.

b) Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsable del tratamiento.

c) Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.

3. En el supuesto contemplado en el apartado anterior, la entidad que encargue la realización de la campaña publicitaria deberá adoptar las medidas necesarias para asegurarse de que la entidad contratada ha recabado los datos cumpliendo las exigencias establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

4. A los efectos previstos en este artículo, se consideran parámetros identificativos de los destinatarios las variables utilizadas para identificar el público objetivo o destinatario de una

campaña o promoción comercial de productos o servicios que permitan acotar los destinatarios individuales de la misma.

Artículo 47. *Depuración de datos personales.*

Cuando dos o más responsables por sí mismos o mediante encargo a terceros pretendieran constatar sin consentimiento de los afectados, con fines de promoción o comercialización de sus productos o servicios y mediante un tratamiento cruzado de sus ficheros quiénes ostentan la condición de clientes de una u otra o de varios de ellos, el tratamiento así realizado constituirá una cesión o comunicación de datos.

Artículo 48. *Ficheros de exclusión del envío de comunicaciones comerciales.*

Los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

Artículo 49. *Ficheros comunes de exclusión del envío de comunicaciones comerciales.*

1. Será posible la creación de ficheros comunes, de carácter general o sectorial, en los que sean objeto de tratamiento los datos de carácter personal que resulten necesarios para evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad.

A tal efecto, los citados ficheros podrán contener los mínimos datos imprescindibles para identificar al afectado.

2. Cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, aquél deberá ser informado de la existencia de los ficheros comunes de exclusión generales o sectoriales, así como de la identidad de su responsable, su domicilio y la finalidad del tratamiento.

El afectado podrá solicitar su exclusión respecto de un fichero o tratamiento concreto o su inclusión en ficheros comunes de excluidos de carácter general o sectorial.

3. La entidad responsable del fichero común podrá tratar los datos de los interesados que hubieran manifestado su negativa u oposición al tratamiento de sus datos con fines de publicidad o prospección comercial, cumpliendo las restantes obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento.

4. Quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán previamente consultar los ficheros comunes que pudieran afectar a su actuación, a fin de evitar que sean objeto de tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa a ese tratamiento.

Artículo 50. *Derechos de acceso, rectificación y cancelación.*

1. El ejercicio de los derechos de acceso, rectificación y cancelación en relación con los tratamientos vinculados a actividades de publicidad y prospección comercial se someterá a lo previsto en los capítulos I a IV del título III de este reglamento.

2. Si el derecho se ejercitase ante una entidad que hubiese encargado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo otorgue al afectado su derecho en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 51. *Derecho de oposición.*

1. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del

tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

La oposición a la que se refiere el párrafo anterior deberá entenderse sin perjuicio del derecho del interesado a revocar cuando lo estimase oportuno el consentimiento que hubiera otorgado, en su caso, para el tratamiento de los datos.

2. A tal efecto, deberá concederse al interesado un medio sencillo y gratuito para oponerse al tratamiento. En particular, se considerará cumplido lo dispuesto en este precepto cuando los derechos puedan ejercitarse mediante la llamada a un número telefónico gratuito o la remisión de un correo electrónico.

3. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a sus clientes o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, deberá concederse la posibilidad al afectado de ejercer su oposición a través de dichos servicios.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar su oposición el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

En todo caso, el ejercicio por el afectado de sus derechos no podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

4. Si el derecho de oposición se ejercitase ante una entidad que hubiera encomendado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo atienda el derecho del afectado en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

TÍTULO V

Obligaciones previas al tratamiento de los datos

CAPÍTULO I

Creación, modificación o supresión de ficheros de titularidad pública

Artículo 52. *Disposición o Acuerdo de creación, modificación o supresión del fichero.*

1. La creación, modificación o supresión de los ficheros de titularidad pública sólo podrá hacerse por medio de disposición general o acuerdo publicados en el «Boletín Oficial del Estado» o diario oficial correspondiente.

2. En todo caso, la disposición o acuerdo deberá dictarse y publicarse con carácter previo a la creación, modificación o supresión del fichero.

Artículo 53. *Forma de la disposición o acuerdo.*

1. Cuando la disposición se refiera a los órganos de la Administración General del Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de orden ministerial o resolución del titular de la entidad u organismo correspondiente.

2. En el caso de los órganos constitucionales del Estado, se estará a lo que establezcan sus normas reguladoras.

3. En relación con los ficheros de los que sean responsables las comunidades autónomas, entidades locales y las entidades u organismos vinculados o dependientes de las mismas, las universidades públicas, así como los órganos de las comunidades

autónomas con funciones análogas a los órganos constitucionales del Estado, se estará a su legislación específica.

4. La creación, modificación o supresión de los ficheros de los que sean responsables las corporaciones de derecho público y que se encuentren relacionados con el ejercicio por aquéllas de potestades de derecho público deberá efectuarse a través de acuerdo de sus órganos de gobierno, en los términos que establezcan sus respectivos Estatutos, debiendo ser igualmente objeto de publicación en el «Boletín Oficial del Estado» o diario oficial correspondiente.

Artículo 54. *Contenido de la disposición o acuerdo.*

1. La disposición o acuerdo de creación del fichero deberá contener los siguientes extremos:

a) La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.

b) El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.

c) La estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.

d) Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.

e) Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.

f) Los órganos responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente reglamento.

2. La disposición o acuerdo de modificación del fichero deberá indicar las modificaciones producidas en cualquiera de los extremos a los que se refiere el apartado anterior.

3. En las disposiciones o acuerdos que se dicten para la supresión de los ficheros se establecerá el destino que vaya a darse a los datos o, en su caso, las previsiones que se adopten para su destrucción.

CAPÍTULO II

Notificación e inscripción de los ficheros de titularidad pública o privada

Artículo 55. *Notificación de ficheros.*

1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.

2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.

3. Cuando la obligación de notificar afecte a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos.

El Registro General de Protección de Datos podrá solicitar de las autoridades de control de las comunidades autónomas el traslado al que se refiere el párrafo anterior, procediendo, en su defecto, a la inclusión de oficio del fichero en el Registro.

4. La notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

Artículo 56. *Tratamiento de datos en distintos soportes.*

1. La notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento de los datos.

2. Cuando los datos de carácter personal objeto de un tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado sólo será precisa una sola notificación, referida a dicho fichero.

Artículo 57. *Ficheros en los que exista más de un responsable.*

Cuando se tenga previsto crear un fichero del que resulten responsables varias personas o entidades simultáneamente, cada una de ellas deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las comunidades autónomas, la creación del correspondiente fichero.

Artículo 58. *Notificación de la modificación o supresión de ficheros.*

1. La inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la Agencia Española de Protección de Datos o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción en el registro correspondiente, conforme a lo dispuesto en el artículo 55.

2. Cuando el responsable del fichero decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el registro correspondiente.

3. Tratándose de ficheros de titularidad pública, cuando se pretenda la modificación que afecte a alguno de los requisitos previstos en el artículo 55 o la supresión del fichero deberá haberse adoptado, con carácter previo a la notificación la correspondiente norma o acuerdo en los términos previstos en el capítulo I de este título.

Artículo 59. *Modelos y soportes para la notificación.*

1. La Agencia Española de Protección de Datos publicará mediante la correspondiente Resolución del Director los modelos o formularios electrónicos de notificación de creación, modificación o supresión de ficheros, que permitan su presentación a través de medios telemáticos o en soporte papel, así como, previa consulta de las autoridades de protección de datos de las comunidades autónomas, los formatos para la comunicación telemática de ficheros públicos por las autoridades de control autonómicas, de conformidad con lo establecido en los artículos 55 y 58 del presente reglamento.

2. Los modelos o formularios electrónicos de notificación se podrán obtener gratuitamente en la página web de la Agencia Española de Protección de Datos.

3. El Director de la Agencia Española de Protección de Datos podrá establecer procedimientos simplificados de notificación en atención a las circunstancias que concurran en el tratamiento o el tipo de fichero al que se refiera la notificación.

Artículo 60. *Inscripción de los ficheros.*

1. El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución acordando, en su caso, la inscripción, una vez tramitado el procedimiento previsto en el capítulo IV del título IX.

2. La inscripción contendrá el código asignado por el Registro, la identificación del responsable del fichero, la identificación del fichero o tratamiento, la descripción de su finalidad y usos previstos, el sistema de tratamiento empleado en su organización, en su caso, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, y la indicación del nivel de medidas de seguridad exigible conforme a lo dispuesto en el artículo 81.

Asimismo, se incluirán, en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales.

En el caso de ficheros de titularidad pública también se hará constar la referencia de la disposición general por la que ha sido creado, y en su caso, modificado.

3. La inscripción de un fichero en el Registro General de Protección de Datos, no exime al responsable del cumplimiento del resto de las obligaciones previstas en la Ley Orgánica 15/1999, de 13 de diciembre, y demás disposiciones reglamentarias.

Artículo 61. *Cancelación de la inscripción.*

1. Cuando el responsable del tratamiento comunicase, en virtud de lo dispuesto en el artículo 58 de este reglamento, la supresión del fichero, el Director de la Agencia Española de Protección de Datos, previa la tramitación del procedimiento establecido en la sección primera del capítulo IV del título IX, dictará resolución acordando la cancelación de la inscripción correspondiente al fichero.

2. El Director de la Agencia Española de Protección de Datos podrá, en ejercicio de sus competencias, acordar de oficio la cancelación de la inscripción de un fichero cuando concurran circunstancias que acrediten la imposibilidad de su existencia, previa la tramitación del procedimiento establecido en la sección segunda del capítulo IV del título IX de este reglamento.

Artículo 62. *Rectificación de errores.*

El Registro General de Protección de Datos podrá rectificar en cualquier momento, de oficio o a instancia de los interesados, los errores materiales, de hecho o aritméticos que pudieran existir en las inscripciones, de conformidad con lo dispuesto en el artículo 105 de la Ley 30/1992, de 26 de noviembre.

Artículo 63. *Inscripción de oficio de ficheros de titularidad pública.*

1. En supuestos excepcionales con el fin de garantizar el derecho a la protección de datos de los afectados, y sin perjuicio de la obligación de notificación, se podrá proceder a la inscripción de oficio de un determinado fichero en el Registro General de Protección de Datos.

2. Para que lo dispuesto en el apartado anterior resulte de aplicación, será requisito indispensable que la correspondiente norma o acuerdo regulador de los ficheros que contengan datos de carácter personal haya sido publicado en el correspondiente diario oficial y cumpla los requisitos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

3. El Director de la Agencia Española de Protección de Datos podrá, a propuesta del Registro General de Protección de Datos, acordar la inscripción del fichero de titularidad pública en el Registro, notificándose dicho acuerdo al órgano responsable del fichero.

Cuando la inscripción se refiera a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, se comunicará a la referida autoridad de control autonómica para que proceda, en su caso, a la inscripción de oficio.

Artículo 64. *Colaboración con las autoridades de control de las comunidades autónomas.*

El Director de la Agencia Española de Protección de Datos podrá celebrar con los directores de las autoridades de control de las comunidades autónomas los convenios de colaboración o acuerdos que estime pertinentes, a fin de garantizar la inscripción en el Registro General de Protección de Datos de los ficheros sometidos a la competencia de dichas autoridades autonómicas.

TÍTULO VI

Transferencias internacionales de datos

CAPÍTULO I

Disposiciones generales

Artículo 65. *Cumplimiento de las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre.*

La transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

Artículo 66. *Autorización y notificación.*

1. Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del presente reglamento.

La autorización se otorgará conforme al procedimiento establecido en la sección primera del capítulo V del título IX de este reglamento.

2. La autorización no será necesaria:

a) Cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección conforme a lo previsto en el capítulo II de este título.

b) Cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a) a j) del artículo 34 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

CAPÍTULO II

Transferencias a estados que proporcionen un nivel adecuado de protección

Artículo 67. *Nivel adecuado de protección acordado por la Agencia Española de Protección de Datos.*

1. No será precisa autorización del Director de la Agencia Española de Protección de Datos a una transferencia internacional de datos cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de protección a juicio del Director de la Agencia Española de Protección de Datos.

El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el

país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se acordase que un determinado país proporciona un nivel adecuado de protección de datos serán publicadas en el «Boletín Oficial del Estado».

2. El Director de la Agencia Española de Protección de Datos acordará la publicación de la relación de países cuyo nivel de protección haya sido considerado equiparable conforme a lo dispuesto en el apartado anterior.

Esta lista se publicará y mantendrá actualizada asimismo a través de medios informáticos o telemáticos.

Artículo 68. *Nivel adecuado de protección declarado por Decisión de la Comisión Europea.*

No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección.

Artículo 69. *Suspensión temporal de las transferencias.*

1. En los supuestos previstos en los artículos precedentes, el Director de la Agencia Española de Protección de Datos, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, podrá acordar, previa audiencia del exportador, la suspensión temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes:

a) Que las autoridades de Protección de Datos del Estado importador o cualquier otra competente, en caso de no existir las primeras, resuelvan que el importador ha vulnerado las normas de protección de datos establecidas en su derecho interno.

b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia Española de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

2. La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

En estos casos, la decisión del Director de la Agencia Española de Protección de Datos será notificada a la Comisión Europea.

CAPÍTULO III

Transferencias a Estados que no proporcionen un nivel adecuado de protección

Artículo 70. *Transferencias sujetas a autorización del Director de la Agencia Española de Protección de Datos.*

1. Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos.

La autorización de la transferencia se tramitará conforme al procedimiento establecido en la sección primera del capítulo V del título IX del presente reglamento.

2. La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

A tal efecto, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de diciembre de 2004 o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

3. En el supuesto contemplado en el apartado anterior, el Director de la Agencia Española de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, suspender temporalmente, previa audiencia del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes:

a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.

b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.

c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.

d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.

e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas a las que se refiere este apartado serán notificadas a la Comisión de las Comunidades Europeas cuando así sea exigible.

4. También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

En este caso, para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español.

En todo caso, la autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento.

TÍTULO VII

Códigos tipo

Artículo 71. *Objeto y naturaleza.*

1. Los códigos tipo a los que se refiere el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, tienen por objeto adecuar lo establecido en la citada Ley Orgánica y en el presente reglamento a las peculiaridades de los tratamientos efectuados por quienes se adhieren a los mismos.

A tal efecto, contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional y serán vinculantes para quienes se adhieran a los mismos.

Artículo 72. *Iniciativa y ámbito de aplicación.*

1. Los códigos tipo tendrán carácter voluntario.

2. Los códigos tipo de carácter sectorial podrán referirse a la totalidad o a parte de los tratamientos llevados a cabo por entidades pertenecientes a un mismo sector, debiendo ser formulados por organizaciones representativas de dicho sector, al menos en su ámbito territorial de aplicación, y sin perjuicio de la potestad de dichas entidades de ajustar el código tipo a sus peculiaridades.

3. Los códigos tipo promovidos por una empresa deberán referirse a la totalidad de los tratamientos llevados a cabo por la misma.

4. Las Administraciones públicas y las corporaciones de Derecho Público podrán adoptar códigos tipo de acuerdo con lo establecido en las normas que les sean aplicables.

Artículo 73. *Contenido.*

1. Los códigos tipo deberán estar redactados en términos claros y accesibles.

2. Los códigos tipo deben respetar la normativa vigente e incluir, como mínimo, con suficiente grado de precisión:

a) La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.

b) Las previsiones específicas para la aplicación de los principios de protección de datos.

c) El establecimiento de estándares homogéneos para el cumplimiento por los adheridos al código de las obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre.

d) El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.

e) La determinación de las cesiones y transferencias internacionales de datos que, en su caso, se prevean, con indicación de las garantías que deban adoptarse.

f) Las acciones formativas en materia de protección de datos dirigidas a quienes los traten, especialmente en cuanto a su relación con los afectados.

g) Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código tipo, en los términos previstos en el artículo 74 de este reglamento.

3. En particular, deberán contenerse en el código:

a) Cláusulas tipo para la obtención del consentimiento de los afectados al tratamiento o cesión de sus datos.

b) Cláusulas tipo para informar a los afectados del tratamiento, cuando los datos no sean obtenidos de los mismos.

c) Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.

d) Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso.

Artículo 74. *Compromisos adicionales.*

1. Los códigos tipo podrán incluir cualquier otro compromiso adicional que asuman los adheridos para un mejor cumplimiento de la legislación vigente en materia de protección de datos.

2. Además podrán contener cualquier otro compromiso que puedan establecer las entidades promotoras y, en particular, sobre:

a) La adopción de medidas de seguridad adicionales a las exigidas por la Ley Orgánica 15/1999, de 13 de diciembre, y el presente Reglamento.

b) La identificación de las categorías de cesionarios o importadores de los datos.

c) Las medidas concretas adoptadas en materia de protección de los menores o de determinados colectivos de afectados.

d) El establecimiento de un sello de calidad que identifique a los adheridos al código.

Artículo 75. *Garantías del cumplimiento de los códigos tipo.*

1. Los códigos tipo deberán incluir procedimientos de supervisión independientes para garantizar el cumplimiento de las obligaciones asumidas por los adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio.

2. El procedimiento que se prevea deberá garantizar:

a) La independencia e imparcialidad del órgano responsable de la supervisión.

b) La sencillez, accesibilidad, celeridad y gratuidad para la presentación de quejas y reclamaciones ante dicho órgano por los eventuales incumplimientos del código tipo.

c) El principio de contradicción.

d) Una graduación de sanciones que permita ajustarlas a la gravedad del incumplimiento. Esas sanciones deberán ser disuasorias y podrán implicar la suspensión de la adhesión al código o la expulsión de la entidad adherida. Asimismo, podrá establecerse, en su caso, su publicidad.

e) La notificación al afectado de la decisión adoptada.

3. Asimismo, y sin perjuicio de lo dispuesto en el artículo 19 de la Ley Orgánica 15/1999, de 13 de diciembre, los códigos tipo podrán contemplar procedimientos para la determinación de medidas reparadoras en caso de haberse causado un perjuicio a los afectados como consecuencia del incumplimiento del código tipo.

4. Lo dispuesto en este artículo se aplicará sin perjuicio de las competencias de la Agencia Española de Protección de Datos y, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 76. *Relación de adheridos.*

El código tipo deberá incorporar como anexo una relación de adheridos, que deberá mantenerse actualizada, a disposición de la Agencia Española de Protección de Datos.

Artículo 77. *Depósito y publicidad de los códigos tipo.*

1. Para que los códigos tipo puedan ser considerados como tales a los efectos previstos en el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento, deberán ser depositados e inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos o, cuando corresponda, en el registro que fuera creado por las comunidades autónomas, que darán traslado para su inclusión al Registro General de Protección de Datos.

2. A tal efecto, los códigos tipo deberán ser presentados ante la correspondiente autoridad de control, tramitándose su inscripción, en caso de estar sometidos a la decisión de la Agencia Española de Protección de Datos, conforme al procedimiento establecido en el capítulo VI del título IX de este reglamento.

3. En todo caso, la Agencia Española de Protección de Datos dará publicidad a los códigos tipo inscritos, preferentemente a través de medios informáticos o telemáticos.

Artículo 78. *Obligaciones posteriores a la inscripción del código tipo.*

Las entidades promotoras o los órganos, personas o entidades que al efecto se designen en el propio código tipo tendrán, una vez el mismo haya sido publicado, las siguientes obligaciones:

a) Mantener accesible al público la información actualizada sobre las entidades promotoras, el contenido del código tipo, los procedimientos de adhesión y de garantía de su cumplimiento y la relación de adheridos a la que se refiere el artículo anterior.

Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos.

b) Remitir a la Agencia Española de Protección de Datos una memoria anual sobre las actividades realizadas para difundir el código tipo y promover la adhesión a éste, las actuaciones de verificación del cumplimiento del código y sus resultados, las quejas y reclamaciones tramitadas y el curso que se les hubiera dado y cualquier otro aspecto que las entidades promotoras consideren adecuado destacar.

Cuando se trate de códigos tipo inscritos en el registro de una autoridad de control de una comunidad autónoma, la remisión se realizará a dicha autoridad, que dará traslado al registro General de Protección de Datos.

c) Evaluar periódicamente la eficacia del código tipo, midiendo el grado de satisfacción de los afectados y, en su caso, actualizar su contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento.

Esta evaluación deberá tener lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor.

d) Favorecer la accesibilidad de todas las personas, con especial atención a las que tengan alguna discapacidad o de edad avanzada a toda la información disponible sobre el código tipo.

TÍTULO VIII

De las medidas de seguridad en el tratamiento de datos de carácter personal

CAPÍTULO I

Disposiciones generales

Artículo 79. *Alcance.*

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento.

Artículo 80. *Niveles de seguridad.*

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Artículo 81. *Aplicación de los niveles de seguridad.*

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de infracciones administrativas o penales.

b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c) Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Artículo 82. *Encargado del tratamiento.*

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.

Artículo 83. *Prestaciones de servicios sin acceso a datos personales.*

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Artículo 84. *Delegación de autorizaciones.*

Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

Artículo 85. *Acceso a datos a través de redes de comunicaciones.*

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.

Artículo 86. *Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.*

1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 87. *Ficheros temporales o copias de trabajo de documentos.*

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II

Del documento de seguridad

Artículo 88. *El documento de seguridad.*

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el

sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

CAPÍTULO III

Medidas de seguridad aplicables a ficheros y tratamientos automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 89. *Funciones y obligaciones del personal.*

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 90. *Registro de incidencias.*

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 91. *Control de acceso.*

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 92. *Gestión de soportes y documentos.*

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de

medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Artículo 93. *Identificación y autenticación.*

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 94. *Copias de respaldo y recuperación.*

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 95. *Responsable de seguridad.*

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Artículo 96. *Auditoría.*

1. A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 97. *Gestión de soportes y documentos.*

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 98. *Identificación y autenticación.*

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 99. *Control de acceso físico.*

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 100. *Registro de incidencias.*

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 101. *Gestión y distribución de soportes.*

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 102. *Copias de respaldo y recuperación.*

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 103. *Registro de accesos.*

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.

b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Artículo 104. *Telecomunicaciones.*

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPÍTULO IV

Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 105. *Obligaciones comunes.*

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

a) Alcance.
b) Niveles de seguridad.
c) Encargado del tratamiento.
d) Prestaciones de servicios sin acceso a datos personales.
e) Delegación de autorizaciones.
f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
g) Copias de trabajo de documentos.
h) Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:
a) Funciones y obligaciones del personal.
b) Registro de incidencias.
c) Control de acceso.
d) Gestión de soportes.

Artículo 106. *Criterios de archivo.*

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. *Dispositivos de almacenamiento.*

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 108. *Custodia de los soportes.*

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 109. *Responsable de seguridad.*

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. *Auditoría.*

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 111. *Almacenamiento de la información.*

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. *Copia o reproducción.*

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. *Acceso a la documentación.*

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. *Traslado de documentación.*

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

TÍTULO IX

Procedimientos tramitados por la Agencia Española de Protección de Datos

CAPÍTULO I

Disposiciones generales

Artículo 115. *Régimen aplicable.*

1. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el presente título, y supletoriamente, por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. Específicamente serán de aplicación las normas reguladoras del procedimiento administrativo común al régimen de representación en los citados procedimientos.

Artículo 116. *Publicidad de las resoluciones.*

1. La Agencia Española de Protección de Datos hará públicas sus resoluciones, con excepción de las correspondientes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos y de aquéllas por las que se resuelva la inscripción en el mismo de los códigos tipo, siempre que se refieran a procedimientos que se hubieran iniciado con posterioridad al 1 de enero de 2004, o correspondan al archivo de actuaciones inspectoras incoadas a partir de dicha fecha.

2. La publicación de estas resoluciones se realizará preferentemente mediante su inserción en el sitio web de la Agencia Española de Protección de Datos, dentro del plazo de un mes a contar desde la fecha de su notificación a los interesados.

3. En la notificación de las resoluciones se informará expresamente a los interesados de la publicidad prevista en el artículo 37.2 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. La publicación se realizará aplicando los criterios de disociación de los datos de carácter personal que a tal efecto se establezcan mediante Resolución del Director de la Agencia.

CAPÍTULO II

Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición

Artículo 117. *Instrucción del procedimiento.*

1. El procedimiento se iniciará a instancia del afectado o afectados, expresando con claridad el contenido de su reclamación y de los preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, que se consideran vulnerados.

2. Recibida la reclamación en la Agencia Española de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.

3. Recibidas las alegaciones o transcurrido el plazo previsto en el apartado anterior, la Agencia Española de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada.

Artículo 118. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento de tutela de derechos será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la reclamación del afectado o afectados.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su reclamación por silencio administrativo positivo.

Artículo 119. *Ejecución de la resolución.*

Si la resolución de tutela fuese estimatoria, se requerirá al responsable del fichero para que, en el plazo de diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de la tutela, debiendo dar cuenta por escrito de dicho cumplimiento a la Agencia Española de Protección de Datos en idéntico plazo.

CAPÍTULO III

Procedimientos relativos al ejercicio de la potestad sancionadora

Sección 1.ª Disposiciones generales

Artículo 120. *Ámbito de aplicación.*

1. Las disposiciones contenidas en el presente capítulo serán de aplicación a los procedimientos relativos al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora que le viene atribuida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, en la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. No obstante, las disposiciones previstas en el ar-tículo 121 y en la sección cuarta de este capítulo únicamente serán aplicables a los procedimientos referidos al ejercicio de la potestad sancionadora prevista en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 121. *Inmovilización de ficheros.*

1. En el supuesto previsto como infracción muy grave en la Ley Orgánica 15/1999, de 13 de diciembre, consistente en la utilización o cesión ilícita de los datos de carácter personal en la que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia Española de Protección de Datos podrá, en cualquier momento del procedimiento, requerir a los responsables de ficheros o tratamientos de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos.

2. El requerimiento deberá ser atendido en el plazo improrrogable de tres días, durante el cual el responsable del fichero podrá formular las alegaciones que tenga por convenientes en orden al levantamiento de la medida.

3. Si el requerimiento fuera desatendido, el Director de la Agencia Española de Protección de Datos podrá, mediante resolución motivada, acordar la inmovilización de tales ficheros o tratamientos, a los solos efectos de restaurar los derechos de las personas afectadas.

Sección 2.ª Actuaciones previas

Artículo 122. *Iniciación.*

1. Con anterioridad a la iniciación del procedimiento sancionador, se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación del procedimiento, identificar la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso.

2. Las actuaciones previas se llevarán a cabo de oficio por la Agencia Española de Protección de Datos, bien por iniciativa propia o como consecuencia de la existencia de una denuncia o una petición razonada de otro órgano.

3. Cuando las actuaciones se lleven a cabo como consecuencia de la existencia de una denuncia o de una petición razonada de otro órgano, la Agencia Española de Protección de Datos acusará recibo de la denuncia o petición, pudiendo solicitar cuanta documentación se estime oportuna para poder comprobar los hechos susceptibles de motivar la incoación del procedimiento sancionador.

4. Estas actuaciones previas tendrán una duración máxima de doce meses a contar desde la fecha en la que la denuncia o petición razonada a las que se refiere el apartado 2 hubieran tenido entrada en la Agencia Española de Protección de Datos o, en caso de no

existir aquéllas, desde que el Director de la Agencia acordase la realización de dichas actuaciones.

El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previas.

Artículo 123. *Personal competente para la realización de las actuaciones previas.*

1. Las actuaciones previas serán llevadas a cabo por el personal del área de la Inspección de Datos habilitado para el ejercicio de funciones inspectoras.

2. **(Anulado)**

3. Los funcionarios que ejerzan la inspección a los que se refieren los dos apartados anteriores tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 124. *Obtención de información.*

Los inspectores podrán recabar cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal fin podrán requerir la exhibición o el envío de los documentos y datos y examinarlos en el lugar en que se encuentren depositados, como obtener copia de los mismos, inspeccionar los equipos físicos y lógicos, así como requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del fichero o ficheros sujetos a investigación, accediendo a los lugares donde se hallen instalados.

Artículo 125. *Actuaciones presenciales.*

1. En el desarrollo de las actuaciones previas se podrán realizar visitas de inspección por parte de los inspectores designados, en los locales o sede del inspeccionado, o donde se encuentren ubicados los ficheros, en su caso. A tal efecto, los inspectores habrán sido previamente autorizados por el Director de la Agencia Española de Protección de Datos.

Las inspecciones podrán realizarse en el domicilio del inspeccionado, en la sede o local concreto relacionado con el mismo o en cualquiera de sus locales, incluyendo aquéllos en que el tratamiento sea llevado a cabo por un encargado.

La autorización se limitará a indicar la habilitación del inspector autorizado y la identificación de la persona u órgano inspeccionado.

2. En el supuesto contemplado en el apartado anterior, las inspecciones concluirán con el levantamiento de la correspondiente acta, en la que quedará constancia de las actuaciones practicadas durante la visita o visitas de inspección.

3. El acta, que se emitirá por duplicado, será firmada por los inspectores actuantes y por el inspeccionado, que podrá hacer constar en la misma las alegaciones o manifestaciones que tenga por conveniente.

En caso de negativa del inspeccionado a la firma del acta, se hará constar expresamente esta circunstancia en la misma. En todo caso, la firma por el inspeccionado del acta no supondrá su conformidad, sino tan sólo la recepción de la misma.

Se entregará al inspeccionado uno de los originales del acta de inspección, incorporándose el otro a las actuaciones.

Artículo 126. *Resultado de las actuaciones previas.*

1. Finalizadas las actuaciones previas, éstas se someterán a la decisión del Director de la Agencia Española de Protección de Datos.

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

2. En caso de apreciarse la existencia de indicios susceptibles de motivar la imputación de una infracción, el Director de la Agencia Española de Protección de Datos dictará acuerdo de inicio de procedimiento sancionador o de infracción de las Administraciones públicas, que se tramitarán conforme a lo dispuesto, respectivamente, en las secciones tercera y cuarta del presente capítulo.

Sección 3.ª Procedimiento sancionador

Artículo 127. *Iniciación del procedimiento.*

Con carácter específico el acuerdo de inicio del procedimiento sancionador deberá contener:

a) Identificación de la persona o personas presuntamente responsables.

b) Descripción sucinta de los hechos imputados, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.

c) Indicación de que el órgano competente para resolver el procedimiento es el Director de la Agencia Española de Protección de Datos.

d) Indicación al presunto responsable de que puede reconocer voluntariamente su responsabilidad, en cuyo caso se dictará directamente resolución.

e) Designación de instructor y, en su caso, secretario, con expresa indicación del régimen de recusación de los mismos.

f) Indicación expresa del derecho del responsable a formular alegaciones, a la audiencia en el procedimiento y a proponer las pruebas que estime procedentes.

g) Medidas de carácter provisional que pudieran acordarse, en su caso, conforme a lo establecido en la sección primera del presente capítulo.

Artículo 128. *Plazo máximo para resolver.*

1. El plazo para dictar resolución será el que determinen las normas aplicables a cada procedimiento sancionador y se computará desde la fecha en que se dicte el acuerdo de inicio hasta que se produzca la notificación de la resolución sancionadora, o se acredite debidamente el intento de notificación.

2. El vencimiento del citado plazo máximo, sin que se haya dictada y notificada resolución expresa, producirá la caducidad del procedimiento y el archivo de las actuaciones.

Sección 4.ª Procedimiento de declaración de infracción de la Ley Orgánica 15/1999, de 13 de diciembre, por las administraciones públicas

Artículo 129. *Disposición general.*

El procedimiento por el que se declare la existencia de una infracción de la Ley Orgánica 15/1999, de 13 de diciembre, cometida por las Administraciones públicas será el establecido en la sección tercera de este capítulo.

CAPÍTULO IV

Procedimientos relacionados con la inscripción o cancelación de ficheros

Sección 1.ª Procedimiento de inscripción de la creación, modificación o supresión de ficheros

Artículo 130. *Iniciación del procedimiento.*

1. El procedimiento se iniciará como consecuencia de la notificación de la creación, modificación o supresión del fichero por el interesado o, en su caso, de la comunicación efectuada por las autoridades de control de las comunidades autónomas, a la que se refiere el presente reglamento.

2. La notificación se deberá efectuar cumplimentando los modelos o formularios electrónicos publicados al efecto por la Agencia Española de Protección de Datos, en virtud de lo dispuesto en el apartado 1 del artículo 59 de este reglamento.

Tratándose de la notificación de la modificación o supresión de un fichero, deberá indicarse en la misma el código de inscripción del fichero en el Registro General de Protección de Datos.

3. La notificación se efectuará en soporte electrónico, ya mediante comunicación electrónica a través de Internet mediante firma electrónica o en soporte informático, utilizando al efecto el programa de ayuda para la generación de notificaciones que la Agencia pondrá a disposición de los interesados de forma gratuita.

Será igualmente válida la notificación efectuada en soporte papel cuando para su cumplimentación hayan sido utilizados los modelos o formularios publicados por la Agencia.

4. En la notificación, el responsable del fichero deberá declarar un domicilio a efectos de notificaciones en el procedimiento.

Artículo 131. *Especialidades en la notificación de ficheros de titularidad pública.*

1. Cuando se trate de la notificación de ficheros de titularidad pública, deberá acompañarse a la notificación una copia de la norma o acuerdo de creación, modificación o supresión del fichero a que hace referencia el ar-tículo 52 del presente reglamento.

Cuando el diario oficial en el que se encuentre publicada la citada norma o acuerdo sea accesible a través de Internet, bastará con indicar en la notificación la dirección electrónica que permita su concreta localización.

2. Recibida la notificación, si la misma no contuviera la información preceptiva o se advirtieran defectos formales, el Registro General de Protección de Datos requerirá al responsable del fichero para que complete o subsane la notificación. El plazo para la subsanación o mejora de la solicitud será de tres meses, en el caso de que se precise la modificación de la norma o acuerdo de creación del fichero.

Artículo 132. *Acuerdo de inscripción o cancelación.*

Si la notificación referida a la creación, modificación o supresión del fichero contuviera la información preceptiva y se cumplieran las restantes exigencias legales, el Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, acordará, respectivamente, la inscripción del fichero, asignando al mismo el correspondiente código de inscripción, la modificación de la inscripción del fichero o la cancelación de la inscripción correspondiente.

Artículo 133. *Improcedencia o denegación de la inscripción.*

El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución denegando la inscripción, modificación o cancelación cuando de los documentos aportados por el responsable del fichero se desprenda que la notificación no resulta conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

La resolución será debidamente motivada, con indicación expresa de las causas que impiden la inscripción, modificación o cancelación.

Artículo 134. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución acerca de la inscripción, modificación o cancelación será de un mes.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá inscrito, modificado o cancelado el fichero a todos los efectos.

Sección 2.ª Procedimiento de cancelación de oficio de ficheros inscritos

Artículo 135. *Iniciación del procedimiento.*

El procedimiento de cancelación de oficio de los ficheros inscritos en el Registro General de Protección de Datos se iniciará siempre de oficio, bien por propia iniciativa o en virtud de denuncia, por acuerdo del Director de la Agencia Española de Protección de Datos.

Artículo 136. *Terminación del expediente.*

La resolución, previa audiencia del interesado, acordará haber lugar o no a la cancelación del fichero.

Si la resolución acordase la cancelación del fichero, se dará traslado de la misma al Registro General de Protección de Datos, para que proceda a la cancelación.

CAPÍTULO V

Procedimientos relacionados con las transferencias internacionales de datos

Sección 1.ª Procedimiento de autorización de transferencias internacionales de datos

Artículo 137. *Iniciación del procedimiento.*

1. El procedimiento para la obtención de la autorización para las transferencias internacionales de datos a países terceros a las que se refiere el artículo 33 de la Ley Orgánica 15/1999, de 13 de diciembre, y el artículo 70 de este reglamento se iniciará siempre a solicitud del exportador que pretenda llevar a cabo la transferencia.

2. En su solicitud, además de los requisitos legalmente exigidos, el exportador deberá consignar, en todo caso:

a) La identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional, con indicación de su denominación y código de inscripción del fichero en el Registro General de Protección de Datos.

b) La transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica.

c) La documentación que incorpore las garantías exigibles para la obtención de la autorización así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso.

Cuando la autorización se fundamente en la existencia de un contrato entre el exportador y el importador de los datos, deberá aportarse copia del mismo, acreditándose asimismo la concurrencia de poder suficiente en sus otorgantes.

Si la autorización se pretendiera fundar en lo dispuesto en el apartado 4 del artículo 70, deberán aportarse las normas o reglas adoptadas en relación con el tratamiento de los datos en el seno del grupo, así como la documentación que acredite su carácter vinculante y su eficacia dentro del grupo. Igualmente deberá aportarse la documentación que acredite la posibilidad de que el afectado o la Agencia Española de Protección de Datos puedan exigir la responsabilidad que corresponda en caso de perjuicio del afectado o vulneración de las normas de protección de datos por parte de cualquier empresa importadora.

Artículo 138. *Instrucción del procedimiento.*

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha Ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

3. Transcurrido el plazo previsto en el apartado 1, en caso de que se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 139. *Actos posteriores a la resolución.*

1. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la transferencia internacional de datos, se dará traslado de la resolución de autorización al Registro General de Protección de Datos, a fin de proceder a su inscripción.

El Registro General de Protección de Datos inscribirá de oficio la autorización de transferencia internacional.

2. En todo caso, se dará traslado de la resolución de autorización o denegación de la autorización de la transferencia internacional de datos al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 140. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos.

Sección 2.ª Procedimiento de suspensión temporal de transferencias internacionales de datos

Artículo 141. *Iniciación.*

1. En los supuestos contemplados en el artículo 69 y en el apartado 3 del artículo 70, el Director de la Agencia Española de Protección de Datos podrá acordar la suspensión temporal de una transferencia internacional de datos.

2. En tales supuestos, el Director dictará acuerdo de inicio referido a la suspensión temporal de la transferencia. El acuerdo deberá ser motivado y fundarse en los supuestos previstos en este reglamento.

Artículo 142. *Instrucción y resolución.*

1. Se dará traslado del acuerdo al exportador, a fin de que en el plazo de quince días formule lo que a su derecho convenga.

2. Recibidas las alegaciones o cumplido el plazo señalado, el Director dictará resolución acordando, en su caso, la suspensión temporal de la transferencia internacional de datos.

Artículo 143. *Actos posteriores a la resolución.*

1. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el registro.

El Registro General de Protección de Datos inscribirá de oficio la suspensión temporal de la transferencia internacional.

2. En todo caso, se dará traslado de la resolución al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 144. *Levantamiento de la suspensión temporal.*

1. La suspensión se levantará tan pronto como cesen las causas que la hubieran justificado, mediante resolución del Director de la Agencia Española de Protección de Datos, del que se dará traslado al exportador.

2. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el Registro.

El Registro General de Protección de Datos hará constar de oficio el levantamiento de la suspensión temporal de la transferencia internacional.

3. El acuerdo será notificado al exportador y al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26. 3 de la Directiva 95/46/CE.

CAPÍTULO VI

Procedimiento de inscripción de códigos tipo

Artículo 145. *Iniciación del procedimiento.*

1. El procedimiento para la inscripción en el Registro General de Protección de Datos de los códigos tipo se iniciará siempre a solicitud de la entidad, órgano o asociación promotora del código tipo.

2. La solicitud, que deberá reunir los requisitos legalmente establecidos, habrá de acompañarse de los siguientes documentos:

a) Acreditación de la representación que concurra en la persona que presente la solicitud.

b) Contenido del acuerdo, convenio o decisión por la que se aprueba, en el ámbito correspondiente el contenido del código tipo presentado.

c) En caso de que el código tipo proceda de un acuerdo sectorial o una decisión de empresa certificación referida a la adopción del acuerdo y legitimación del órgano que lo adoptó.

d) En el supuesto contemplado en la letra anterior, copia de los estatutos de la asociación, organización sectorial o entidad en cuyo marco haya sido aprobado el código.

e) En caso de códigos tipo presentados por asociaciones u organizaciones de carácter sectorial, documentación relativa a su representatividad en el sector.

f) En caso de códigos tipo basados en decisiones de empresa, descripción de los tratamientos a los que se refiere el código tipo.

g) Código tipo sometido a la Agencia Española de Protección de Datos.

Artículo 146. *Análisis de los aspectos sustantivos del código tipo.*

1. Durante los treinta días siguientes a la notificación o subsanación de los defectos el Registro General de Protección de Datos podrá convocar a los solicitantes, a fin de obtener aclaraciones o precisiones relativas al contenido sustantivo del código tipo.

2. Transcurrido el plazo señalado en el apartado anterior, el Registro General de Protección de Datos elaborará un informe sobre las características del proyecto de código tipo.

3. La documentación presentada y el informe del Registro serán remitidos al Gabinete Jurídico, a fin de que por el mismo se informe acerca del cumplimiento de los requisitos establecidos en el Título VII de este Reglamento.

Artículo 147. *Información pública.*

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

Artículo 148. *Mejora del código tipo.*

Si durante la tramitación del procedimiento resultase necesaria la aportación de nuevos documentos o la modificación del código tipo presentado, la Agencia Española de Protección de Datos podrá requerir al solicitante, a fin de que en el plazo de treinta días introduzca las modificaciones que sean precisas, remitiendo el texto resultante a la Agencia Española de Protección de Datos.

Se declarará la suspensión del procedimiento en tanto el solicitante no dé cumplimiento al requerimiento.

Artículo 149. *Trámite de audiencia.*

En caso de que durante el trámite previsto en el ar-tículo 148 se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 150. *Resolución.*

1. Cumplidos los términos establecidos en los artículos precedentes, el Director de la Agencia resolverá sobre la procedencia o improcedencia de la inscripción del código tipo en el Registro General de Protección de Datos.

2. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la inscripción del código tipo, se dará traslado de la resolución al Registro General de Protección de Datos, a fin de proceder a su inscripción.

Artículo 151. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución será de seis meses, a contar desde la fecha de entrada de la solicitud en la Agencia Española de Protección de Datos.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el solicitante podrá considerar estimada su solicitud.

Artículo 152. *Publicación de los códigos tipo por la Agencia Española de Protección de Datos.*

La Agencia Española de Protección de Datos dará publicidad al contenido de los códigos tipo inscritos en el Registro General de Protección de Datos, utilizando para ello, con carácter preferente, medios electrónicos o telemáticos.

CAPÍTULO VII

Otros procedimientos tramitados por la agencia española de protección de datos

Sección 1.ª Procedimiento de exención del deber de información al interesado

Artículo 153. *Iniciación del procedimiento.*

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la exención del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal cuando resulte imposible o exija esfuerzos desproporcionados, prevista en el apartado 5 del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, se iniciará siempre a petición del responsable que pretenda obtener la aplicación de la exención.

2. En el escrito de solicitud, además de los requisitos recogidos en el art. 70 de la Ley 30/1992, de 26 de noviembre, el responsable deberá:

a) Identificar claramente el tratamiento de datos al que pretende aplicarse la exención del deber de informar.

b) Motivar expresamente las causas en que fundamenta la imposibilidad o el carácter desproporcionado del esfuerzo que implicaría el cumplimiento del deber de informar.

c) Exponer detalladamente las medidas compensatorias que propone realizar en caso de exoneración del cumplimiento del deber de informar.

d) Aportar una cláusula informativa que, mediante su difusión, en los términos que se indiquen en la solicitud, permita compensar la exención del deber de informar.

Artículo 154. *Propuesta de nuevas medidas compensatorias.*

1. Si la Agencia Española de Protección de Datos considerase insuficientes las medidas compensatorias propuestas por el solicitante, podrá acordar la adopción de medidas complementarias o sustitutivas a las propuestas por aquél en su solicitud.

2. Del acuerdo se dará traslado al solicitante, a fin de que exponga lo que a su derecho convenga en el plazo de quince días.

Artículo 155. *Terminación del procedimiento.*

Concluidos los trámites previstos en los artículos precedentes, el Director de la Agencia dictará resolución, concediendo o denegando la exención del deber de informar. La resolución podrá imponer la adopción de las medidas complementarias a las que se refiere el artículo anterior.

Artículo 156. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud por silencio administrativo positivo.

Sección 2.ª Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos

Artículo 157. *Iniciación del procedimiento.*

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la declaración de la concurrencia en un determinado tratamiento de datos de valores históricos, científicos o estadísticos, a los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento, se iniciará siempre a petición del responsable que pretenda obtener la declaración.

2. En el escrito de solicitud, el responsable deberá:

a) Identificar claramente el tratamiento de datos al que pretende aplicarse la excepción.

b) Motivar expresamente las causas que justificarían la declaración.

c) Exponer detalladamente las medidas que el responsable del fichero se propone implantar para garantizar el derecho de los ciudadanos.

3. La solicitud deberá acompañarse de cuantos documentos o pruebas sean necesarios para justificar la existencia de los valores históricos, científicos o estadísticos que fundamentarían la declaración de la Agencia.

Artículo 158. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud.

Disposición adicional única. *Productos de software.*

Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII de este reglamento.

Disposición final única. *Aplicación supletoria.*

En lo no establecido en el capítulo III del título IX serán de aplicación a los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos las disposiciones contenidas en el Reglamento del Procedimiento para el ejercicio de la potestad sancionadora, aprobado por Real Decreto 1398/1993, de 4 de agosto.

§ 4

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

Jefatura del Estado
«BOE» núm. 251, de 19 de octubre de 2007
Última modificación: 10 de mayo de 2014
Referencia: BOE-A-2007-18243

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

PREÁMBULO

I

La aplicación de las nuevas tecnologías desarrolladas en el marco de la sociedad de la información ha supuesto la superación de las formas tradicionales de comunicación, mediante una expansión de los contenidos transmitidos, que abarcan no sólo la voz, sino también datos en soportes y formatos diversos. A su vez, esta extraordinaria expansión en cantidad y calidad ha venido acompañada de un descenso en los costes, haciendo que este tipo de comunicaciones se encuentre al alcance de cualquier persona y en cualquier rincón del mundo.

La naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados, cuando no delictivos.

Precisamente en el marco de este último objetivo se encuadra la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, cuya transposición a nuestro ordenamiento jurídico es el objetivo principal de esta Ley.

El objeto de esta Directiva es establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados. Se entienden por

agentes facultados los miembros de los Cuerpos Policiales autorizados para ello en el marco de una investigación criminal por la comisión de un delito, el personal del Centro Nacional de Inteligencia para llevar a cabo una investigación de seguridad amparada en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal. Se trata, pues, de que todos éstos puedan obtener los datos relativos a las comunicaciones que, relacionadas con una investigación, se hayan podido efectuar por medio de la telefonía fija o móvil, así como por Internet. El establecimiento de esas obligaciones, justificado en aras de proteger la seguridad pública, se ha efectuado buscando el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la privacidad y la intimidad de las comunicaciones.

En este sentido, la Ley es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

En relación con esta última precisión, cabe señalar que la Directiva se refiere, expresamente, a que los datos conservados deberán estar disponibles a los fines de detección o investigación por delitos graves, definidos éstos de acuerdo con la legislación interna de cada Estado miembro.

II

La Ley cuenta con diez artículos que se agrupan en tres capítulos.

El Capítulo I («Disposiciones Generales») se inicia describiendo su objeto, que básicamente se circunscribe a la determinación de la obligación de conservar los datos enumerados en el artículo 3, que se hayan generado o tratado en el marco de una comunicación de telefonía fija o móvil, o realizada a través de una comunicación electrónica de acceso público o mediante una red pública de comunicaciones. Igualmente, se precisan los fines que, exclusivamente, justifican la obligación de conservación, y que se limitan a la detección, investigación y enjuiciamiento de un delito contemplado en el Código Penal o las leyes penales especiales, con los requisitos y cautelas que la propia Ley establece.

En este capítulo también se precisan las limitaciones sobre el tipo de datos a retener, que son los necesarios para identificar el origen y destino de la comunicación, así como la identidad de los usuarios o abonados de ambos, pero nunca datos que revelen el contenido de la comunicación. Igualmente, la Ley impone la obligación de conservación de datos que permitan determinar el momento y duración de una determinada comunicación, su tipo, así como datos necesarios para identificar el equipo de comunicación empleado y, en el caso de utilización de un equipo móvil, los datos necesarios para su localización.

En relación con los sujetos que quedan obligados a conservar los datos, éstos serán los operadores que presten servicios de comunicaciones electrónicas disponibles al público, o que exploten una red pública de comunicaciones electrónicas en España.

La Ley enumera en su artículo 3, de manera precisa y detallada, el listado de datos que quedan sujetos a la obligación de conservación en el marco de las comunicaciones por telefonía fija, móvil o Internet. Estos datos, que, se repite, en ningún caso revelarán el contenido de la comunicación, son los necesarios para identificar el origen y destino de la comunicación, su hora, fecha y duración, el tipo de servicio utilizado y el equipo de comunicación de los usuarios utilizado. En aplicación de las previsiones contenidas en la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, quedan incluidas también en el ámbito de aplicación de la Ley las denominadas llamadas telefónicas infructuosas. Igualmente se incluye la obligación de conservar los elementos que sean suficientes para identificar el momento de activación de los teléfonos que funcionen bajo la modalidad de prepago.

En el Capítulo II («Conservación y cesión de datos») se establecen los límites para efectuar la cesión de datos, el plazo de conservación de los mismos, que será, con carácter general, de doce meses desde que la comunicación se hubiera establecido (si bien reglamentariamente se podrá reducir a seis meses o ampliar a dos años, como permite la Directiva 2006/24/CE), y los instrumentos para garantizar el uso legítimo de los datos conservados, cuya cesión y entrega exclusivamente se podrá efectuar al agente facultado y para los fines establecidos en la Ley, estando cualquier uso indebido sometido a los mecanismos de control de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo. Además, se establecen previsiones específicas respecto al régimen general regulador de los derechos de acceso, rectificación y cancelación de datos contenido en la referida Ley Orgánica 15/1999.

El Capítulo III, al referirse al régimen sancionador, remite, en cuanto a los incumplimientos de las obligaciones de conservación y protección y seguridad de los datos de carácter personal, a la regulación contenida en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Por otro lado, los incumplimientos de la obligación de puesta a disposición de los agentes facultados, en la medida en que las solicitudes estarán siempre amparadas por orden judicial, constituirían la correspondiente infracción penal.

En las disposiciones contenidas en la parte final se incluyen contenidos diversos. Por un lado, y a los efectos de poder establecer instrumentos para controlar el empleo para fines delictivos de los equipos de telefonía móvil adquiridos mediante la modalidad de prepago, se establece, como obligación de los operadores que comercialicen dicho servicio, la llevanza de un registro con la identidad de los compradores.

Por último, la Ley incorpora en las disposiciones finales una modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, para adaptarla al contenido de esta Ley, una referencia a su amparo competencial, una habilitación general al Gobierno para su desarrollo y un período de seis meses para que las operadoras puedan adaptarse a su contenido.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto de la Ley.*

1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

2. Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.

3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas.

Artículo 2. *Sujetos obligados.*

Son destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 3. *Datos objeto de conservación.*

1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:

a) Datos necesarios para rastrear e identificar el origen de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil:

i) Número de teléfono de llamada.
ii) Nombre y dirección del abonado o usuario registrado.

2.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) La identificación de usuario asignada.
ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.
iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.

b) Datos necesarios para identificar el destino de una comunicación:

1.º Con respecto a la telefonía de red fija y a la telefonía móvil:

i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas.
ii) Los nombres y las direcciones de los abonados o usuarios registrados.

2.º Con respecto al correo electrónico por Internet y la telefonía por Internet:

i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.
ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.
2.° Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:

i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.
ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.

d) Datos necesarios para identificar el tipo de comunicación.

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).
2.° Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1.º Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.
2.° Con respecto a la telefonía móvil:

i) Los números de teléfono de origen y destino.
ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.
iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.

iv) La IMSI de la parte que recibe la llamada.

v) La IMEI de la parte que recibe la llamada.

vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.

3.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) El número de teléfono de origen en caso de acceso mediante marcado de números.

ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1.° La etiqueta de localización (identificador de celda) al inicio de la comunicación.

2.° Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley.

CAPÍTULO II

Conservación y cesión de datos

Artículo 4. *Obligación de conservar datos.*

1. Los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta Ley se conserven de conformidad con lo dispuesto en ella, en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones de que se trate.

En ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. La citada obligación de conservación se extiende a los datos relativos a las llamadas infructuosas, en la medida que los datos son generados o tratados y conservados o registrados por los sujetos obligados. Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada.

3. Los datos relativos a las llamadas no conectadas están excluidos de las obligaciones de conservación contenidas en esta Ley. Se entenderá por llamada no conectada aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados.

Artículo 5. *Período de conservación de los datos.*

1. La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

2. Lo dispuesto en el apartado anterior se entiende sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sobre la obligación de conservar datos bloqueados en los supuestos legales de cancelación.

Artículo 6. *Normas generales sobre cesión de datos.*

1. Los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial.

2. La cesión de la información se efectuará mediante formato electrónico únicamente a los agentes facultados, y deberá limitarse a la información que resulte imprescindible para la consecución de los fines señalados en el artículo 1.

A estos efectos, tendrán la consideración de agentes facultados:

a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.

c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

Artículo 7. *Procedimiento de cesión de datos.*

1. Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente.

2. La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados.

3. El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación.

Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro del plazo de 7 días naturales contados a partir de las 8:00 horas del día natural siguiente a aquél en que el sujeto obligado reciba la orden.

Artículo 8. *Protección y seguridad de los datos.*

1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.

3. El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

4. La Agencia Española de Protección de Datos es la autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados en la presente Ley.

Artículo 9. *Excepciones a los derechos de acceso y cancelación.*

1. El responsable del tratamiento de los datos no comunicará la cesión de datos efectuada de conformidad con esta Ley.

2. El responsable del tratamiento de los datos denegará el ejercicio del derecho de cancelación en los términos y condiciones previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Infracciones y sanciones

Artículo 10. *Infracciones y sanciones.*

1. Constituyen infracciones a lo previsto en la presente Ley las siguientes:

a) Es infracción muy grave la no conservación en ningún momento de los datos a los que se refiere el artículo 3.

b) Son infracciones graves:

i) La no conservación reiterada o sistemática de los datos a los que se refiere el artículo 3.

ii) La conservación de los datos por un período inferior al establecido en el artículo 5.

iii) El incumplimiento deliberado de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8.

c) Son infracciones leves:

i) La no conservación de los datos a los que se refiere el artículo 3 cuando no se califique como infracción muy grave o grave.

ii) El incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8, cuando no se califique como infracción grave.

2. A las infracciones previstas en el apartado anterior, a excepción de las indicadas en los apartados 1.b).iii y 1.c).ii de este artículo, les será de aplicación el régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados.

El procedimiento para sancionar las citadas infracciones se iniciará por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar dicho inicio.

En todo caso, se deberá recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador.

3. A las infracciones previstas en los apartados 1.b).iii y 1.c).ii de este artículo les será de aplicación el régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora a la Agencia Española de Protección de Datos.

Disposición adicional única. *Servicios de telefonía mediante tarjetas de prepago.*

1. Los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago, deberán llevar un libro-registro en el que conste la identidad de los clientes que adquieran una tarjeta inteligente con dicha modalidad de pago.

Los operadores informarán a los clientes, con carácter previo a la venta, de la existencia y contenido del registro, de su disponibilidad en los términos expresados en el número siguiente y de los derechos recogidos en el artículo 38.6 de la Ley 32/2003.

La identificación se efectuará mediante documento acreditativo de la personalidad, haciéndose constar en el libro-registro el nombre, apellidos y nacionalidad del comprador, así como el número correspondiente al documento identificativo utilizado y la naturaleza o denominación de dicho documento. En el supuesto de personas jurídicas, la identificación se realizará aportando la tarjeta de identificación fiscal, y se hará constar en el libro-registro la denominación social y el código de identificación fiscal.

2. Desde la activación de la tarjeta de prepago y hasta que cese la obligación de conservación a que se refiere el artículo 5 de esta Ley, los operadores cederán los datos identificativos previstos en el apartado anterior, cuando para el cumplimiento de sus fines les sean requeridos por los agentes facultados, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera.

3. Los datos identificativos estarán sometidos a las disposiciones de esta Ley, respecto a los sistemas que garanticen su conservación, no manipulación o acceso ilícito, destrucción, cancelación e identificación de la persona autorizada.

4. Los operadores deberán ceder los datos identificativos previstos en el apartado 1 de esta disposición a los agentes facultados, a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, o al personal del Centro Nacional de Inteligencia, así como a los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, cuando les sean requeridos por éstos con fines de investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales.

5. Constituyen infracciones a lo previsto en la presente disposición, además de la previstas en el artículo 10, las siguientes:

a) Es infracción muy grave el incumplimiento de la llevanza del libro-registro referido.

b) Son infracciones graves la llevanza reiterada o sistemáticamente incompleta de dicho libro-registro así como el incumplimiento deliberado de la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición.

c) Son infracciones leves la llevanza incompleta del libro-registro o el incumplimiento de la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición cuando no se califiquen como infracciones muy graves o graves.

6. A las infracciones previstas en el apartado anterior les será de aplicación el régimen sancionador establecido en la Ley 32/2003, de 3 de noviembre, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

El procedimiento para sancionar las citadas infracciones se iniciará por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar dicho inicio.

En todo caso, se deberá recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador.

7. La obligación de inscripción en el libro-registro de los datos identificativos de los compradores que adquieran tarjetas inteligentes, así como el resto de obligaciones contenidas en la presente disposición adicional, comenzarán a ser exigibles a partir de la entrada en vigor de esta Ley.

8. No obstante, por lo que se refiere a las tarjetas adquiridas con anterioridad a la entrada en vigor de esta Ley, los operadores de telefonía móvil que comercialicen estos servicios dispondrán de un plazo de dos años, a contar desde dicha entrada en vigor, para cumplir con las obligaciones de inscripción a que se refiere el apartado 1 de la presente disposición adicional.

Transcurrido el aludido plazo de dos años, los operadores vendrán obligados a anular o a desactivar aquellas tarjetas de prepago respecto de las que no se haya podido cumplir con las obligaciones de inscripción del referido apartado 1 de esta disposición adicional, sin perjuicio de la compensación que, en su caso, corresponda al titular de las mismas por el saldo pendiente de consumo.

Disposición transitoria única. *Vigencia del régimen de interceptación de telecomunicaciones.*

Las normas dictadas en desarrollo del Capítulo III del Título III de la Ley 32/2003, de 3 de noviembre, continuarán en vigor en tanto no se opongan a lo dispuesto en esta Ley.

Disposición derogatoria única. *Derogación normativa.*

1. Quedan derogados los artículos 12, 38.2 c) y d) y 38.3 a) de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
2. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley.

Disposición final primera. *Modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.*

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se modifica en los siguientes términos:

Uno. El artículo 33 queda redactado de la siguiente forma:

«Artículo 33. *Secreto de las comunicaciones.*

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.
2. Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.
3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, este podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.
4. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad o identidades del sujeto objeto de la medida de la interceptación.

Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada

mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica.

c) Servicios básicos utilizados.

d) Servicios suplementarios utilizados.

e) Dirección de la comunicación.

f) Indicación de respuesta.

g) Causa de finalización.

h) Marcas temporales.

i) Información de localización.

j) Información intercambiada a través del canal de control o señalización.

6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) Identificación de la persona física o jurídica.

b) Domicilio en el que el proveedor realiza las notificaciones.

Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:

c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).

d) Número de identificación del terminal.

e) Número de cuenta asignada por el proveedor de servicios Internet.

f) Dirección de correo electrónico.

7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.

8. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.

9. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio.

10. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.

Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.»

Dos. El último párrafo del apartado 5 del artículo 38 pasa a tener la siguiente redacción:

«Lo establecido en las letras a) y d) del apartado 3 de este artículo se entiende sin perjuicio de las obligaciones establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

Tres. En el artículo 53, se modifican los párrafos o) y z), que quedan redactados de la siguiente forma:

«o) El incumplimiento deliberado, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de esta Ley y el incumplimiento deliberado de las obligaciones de conservación de los datos establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

«z) La vulneración grave o reiterada de los derechos previstos en el artículo 38.3, salvo el previsto por el párrafo h), cuya infracción se regirá por el régimen sancionador previsto en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y el incumplimiento grave o reiterado de las obligaciones de protección y seguridad de los datos almacenados establecidas en el artículo 8 de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.»

Cuatro. En el artículo 54 se modifican los párrafos ñ) y r), que quedan redactados de la siguiente forma:

«ñ) El incumplimiento, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de la presente Ley y el incumplimiento de las obligaciones de conservación de los datos establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, salvo que deban considerarse como infracción muy grave, conforme a lo dispuesto en el artículo anterior.»

«r) La vulneración de los derechos previstos en el artículo 38.3, salvo el previsto por el párrafo h), cuya infracción se regirá por el régimen sancionador previsto en la Ley 34/2002, de 11 de julio, y el incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8 de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, salvo que deban considerarse como infracción muy grave.»

Disposición final segunda. *Competencia estatal.*

Esta Ley se dicta al amparo de lo dispuesto en el artículo 149.1.29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública, y del artículo 149.1.21.ª, que confiere al Estado competencia exclusiva en materia de telecomunicaciones.

Disposición final tercera. *Desarrollo reglamentario.*

Se habilita al Gobierno a dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo previsto en esta Ley.

Disposición final cuarta. *Formato de entrega de los datos.*

1. La cesión a los agentes facultados de los datos cuya conservación sea obligatoria, se efectuará en formato electrónico, en la forma que se determine por Orden conjunta de los

Ministros de Interior, de Defensa y de Economía y Hacienda, que se aprobará en el plazo de tres meses desde la entrada en vigor de esta Ley.

2. Los sujetos obligados a los que se refiere el artículo 2 de esta Ley, tendrán un plazo de seis meses desde la entrada en vigor de la misma para configurar, a su costa, sus equipos y estar técnicamente en disposición de cumplir con las obligaciones de conservación y cesión de datos.

Disposición final quinta. *Entrada en vigor.*

Esta Ley entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

§ 5

Resolución de 22 de junio de 2001, de la Subsecretaría, por la que se dispone la publicación del Acuerdo de Consejo de Ministros por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información

Ministerio de Justicia
«BOE» núm. 151, de 25 de junio de 2001
Última modificación: sin modificaciones
Referencia: BOE-A-2001-12222

El Consejo de Ministros, en su reunión de 22 de junio de 2001, ha aprobado el Acuerdo por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información.

Con el fin de favorecer su conocimiento y aplicación generales, se ordena su publicación como anexo a la presente Resolución.

ANEXO

Acuerdo por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información

El Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, establece en su disposición transitoria única los plazos de implantación de las medidas de seguridad para los sistemas de información que se encontraban en funcionamiento a la entrada en vigor de dicho Reglamento, que se produjo el 26 de junio de 1999.

Dicha disposición transitoria única contempla un plazo de dos años para que se proceda a la implantación de las medidas de seguridad de nivel alto en los indicados sistemas de información, si bien la propia norma prevé la ampliación en un año del plazo inicial, cuando los sistemas de información que se encuentren en funcionamiento no permitan tecnológicamente la implantación de alguna de las medidas de seguridad a las que se refiere el Reglamento.

El 26 de junio de 2001 se cumplen dos años desde la entrada en vigor del Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal y resulta constatable que respecto de numerosos sistemas de información, tanto de titularidad pública como privada, que ya se encontraban en funcionamiento en aquella fecha y en los cuales, de acuerdo con lo previsto en el artículo 4.3 del Reglamento, deben implantarse las medidas de seguridad calificadas como de nivel alto que se determinan en su capítulo IV, se han encontrado dificultades de orden tecnológico que han imposibilitado la plena implantación de tales medidas hasta el momento.

En virtud de ello parece oportuno, apreciando que concurren las circunstancias previstas para la aplicación del párrafo segundo de la disposición transitoria única del Reglamento, hacer uso de la facultad de ampliar el plazo para la implantación de las medidas de seguridad de nivel alto en los sistemas de información que estuvieran en funcionamiento antes de la entrada en vigor de aquél, que será, en consecuencia, de tres años a contar de dicha fecha.

Por todo lo cual, a propuesta del Ministro de Justicia, previo informe de la Agencia de Protección de Datos, el Consejo de Ministros, en su reunión del día 22 de junio de 2001, acuerda:

El plazo para la implantación de las medidas de seguridad de nivel alto en aquellos sistemas de información que se hallaban en funcionamiento con anterioridad a la fecha de entrada en vigor del Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, será de tres años desde la citada fecha de entrada en vigor, concluyendo, en consecuencia, el 26 de junio de 2002.

§ 6

Orden de 2 de febrero de 1995 por la que se aprueba la primera relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos

Ministerio de Justicia e Interior
«BOE» núm. 35, de 10 de febrero de 1995
Última modificación: 21 de agosto de 1998
Referencia: BOE-A-1995-3543

La transferencia internacional de datos se regula en los artículos 32 y 33 de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, y se completa en los artículos 3 y 4 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de dicha Ley, cuya disposición final primera faculta al Ministro de Justicia e Interior para aprobar la relación de países que, a efectos de lo dispuesto en el artículo 32 de la propia Ley Orgánica, se entiende que proporcionan un nivel de protección equiparable al de dicha Ley.

Las legislaciones de los distintos países son heterogéneas y difícilmente comparables, por lo cual la relación que se aprueba por la presente Orden deben integrarse por varias relaciones parciales, especificando de forma separada los países que proporcionan un nivel de protección equiparable al español, según se trate de ficheros de titularidad pública o de ficheros de titularidad privada.

Por otra parte, tanto las legislaciones de los distintos países como los estudios que se llevan a cabo en España sobre su naturaleza y alcance, se encuentran en un proceso de evolución permanente, por cuya razón lo que se aprueba a través de la presente Orden es una primera relación de países, es decir una relación de carácter abierto, que deberá ser continuada y completada, en paralelo con la evolución de las legislaciones extranjeras y de los estudios correspondientes.

En su virtud, y de conformidad con el preceptivo informe emitido por el Director de la Agencia de Protección de Datos, dispongo:

Primero.

Los países cuyo régimen legal de protección de datos de carácter personal, objeto de tratamiento automatizado, se considera que proporciona un nivel de protección equiparable al de la Ley Orgánica 5/1992, de 29 de octubre, tanto respecto a ficheros de titularidad pública como a los de titularidad privada, son los países parte del Convenio para la Protección de las Personas con relación al Tratamiento Automatizado de los Datos de Carácter Personal, abierto a la firma en Estrasburgo el 28 de enero de 1981, y concretamente los siguientes:

Alemania, Austria, Bélgica, Dinamarca —con la excepción del territorio de las Islas Féroe y de Groenlandia—, Eslovenia, Finlandia, Francia, Grecia, Irlanda, Italia, Islandia, Luxemburgo, Noruega —con la excepción del territorio de Svalbard—, Países Bajos, Portugal, Reino Unido —inclusive el territorio de las Islas de Man y Jersey— y Suecia.

Segundo.

Asimismo se considera que proporcionan un nivel de protección equiparable al de la Ley Orgánica 5/1992, de 29 de octubre, respecto a ficheros de titularidad pública y de titularidad privada, Australia, Israel, Hungría, Nueva Zelanda, República Checa, República de Slovakia, San Marino y Suiza.

Tercero.

Se considera que proporcionan un nivel de protección equiparable al de la Ley Orgánica 5/1992, de 29 de octubre, respecto de los datos registrados en ficheros de titularidad pública, la República de Andorra y Japón.

Cuarto.

También se considera que proporciona un nivel de protección equiparable al de la Ley Orgánica 5/1992, de 29 de octubre, la legislación de Canadá respecto de los ficheros de titularidad pública, y que disponen de un régimen de protección equiparable al de dicha Ley, respecto de los ficheros de titularidad privada, las provincias canadienses de Quebec, Ontario, Saskatchewan y Columbia Británica.

Quinto.

De conformidad con lo dispuesto en los artículos 32 y 33 de la Ley Orgánica 5/1992, de 29 de octubre, y 3 y 4 del Real Decreto 1332/1994, de 20 de junio, lo dispuesto en la presente Orden se entiende sin perjuicio de lo establecido en tratados o convenios en los que sea parte España, y de las restantes excepciones legales, así como de las facultades que corresponden a la Agencia de Protección de Datos para autorizar las transferencias internacionales de datos, si se obtienen garantías adecuadas.

Disposición final.

La presente Orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 7

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Unión Europea
«DOUE» núm. 119, de 4 de mayo de 2016
Última modificación: sin modificaciones
Referencia: DOUE-L-2016-89807

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 16,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de texto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo [1],

Visto el dictamen del Comité de las Regiones [2],

De conformidad con el procedimiento legislativo ordinario [3],

Considerando lo siguiente:

(1) La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

(2) Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas.

(3) La Directiva 95/46/CE del Parlamento Europeo y del Consejo [4] trata de armonizar la protección de los derechos y las libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal y garantizar la libre circulación de estos datos entre los Estados miembros.

(4) El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe

considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística.

(5) La integración económica y social resultante del funcionamiento del mercado interior ha llevado a un aumento sustancial de los flujos transfronterizos de datos personales. En toda la Unión se ha incrementado el intercambio de datos personales entre los operadores públicos y privados, incluidas las personas físicas, las asociaciones y las empresas. El Derecho de la Unión insta a las autoridades nacionales de los Estados miembros a que cooperen e intercambien datos personales a fin de poder cumplir sus funciones o desempeñar otras por cuenta de una autoridad de otro Estado miembro.

(6) La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

(7) Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.

(8) En los casos en que el presente Reglamento establece que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, estos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del presente Reglamento.

(9) Aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada, ni la inseguridad jurídica ni una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas físicas, en particular en relación con las actividades en línea. Las diferencias en el nivel de protección de los derechos y libertades de las personas físicas, en particular del derecho a la protección de los datos de carácter personal, en lo que respecta al tratamiento de dichos datos en los Estados miembros pueden impedir la libre circulación de los datos de carácter personal en la Unión. Estas diferencias pueden constituir, por lo tanto, un obstáculo al ejercicio de las actividades económicas a nivel de la Unión, falsear la competencia e impedir que las autoridades cumplan las funciones que les incumben en virtud del Derecho de la Unión. Esta diferencia en los niveles de protección se debe a la existencia de divergencias en la ejecución y aplicación de la Directiva 95/46/CE.

(10) Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea. En lo que respecta al tratamiento de datos personales para el cumplimiento de una obligación legal, para el cumplimiento de una misión

realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los Estados miembros deben estar facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del presente Reglamento. Junto con la normativa general y horizontal sobre protección de datos por la que se aplica la Directiva 95/46/CE, los Estados miembros cuentan con distintas normas sectoriales específicas en ámbitos que precisan disposiciones más específicas. El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito.

(11) La protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes.

(12) El artículo 16, apartado 2, del TFUE encomienda al Parlamento Europeo y al Consejo que establezcan las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal y las normas relativas a la libre circulación de dichos datos.

(13) Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros. El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Con objeto de tener en cuenta la situación específica de las microempresas y las pequeñas y medianas empresas, el presente Reglamento incluye una serie de excepciones en materia de llevanza de registros para organizaciones con menos de 250 empleados. Además, alienta a las instituciones y órganos de la Unión y a los Estados miembros y a sus autoridades de control a tener en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas en la aplicación del presente Reglamento. El concepto de microempresas y pequeñas y medianas empresas debe extraerse del artículo 2 del anexo de la Recomendación 2003/361/CE de la Comisión [(5)].

(14) La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.

(15) A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento.

(16) El presente Reglamento no se aplica a cuestiones de protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con

actividades excluidas del ámbito de del Derecho de la Unión, como las actividades relativas a la seguridad nacional. Tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión.

(17) El Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo [6] se aplica al tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal deben adaptarse a los principios y normas establecidos en el presente Reglamento y aplicarse a la luz del mismo. A fin de establecer un marco sólido y coherente en materia de protección de datos en la Unión, una vez adoptado el presente Reglamento deben introducirse las adaptaciones necesarias del Reglamento (CE) n.º 45/2001, con el fin de que pueda aplicarse al mismo tiempo que el presente Reglamento.

(18) El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

(19) La protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención, es objeto de un acto jurídico específico a nivel de la Unión. El presente Reglamento no debe, por lo tanto, aplicarse a las actividades de tratamiento destinadas a tales fines. No obstante, los datos personales tratados por las autoridades públicas en aplicación del presente Reglamento deben, si se destinan a tales fines, regirse por un acto jurídico de la Unión más específico, concretamente la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo [7]. Los Estados miembros pueden encomendar a las autoridades competentes, tal como se definen en la Directiva (UE) 2016/680, funciones que no se lleven a cabo necesariamente con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluida la protección frente a las amenazas a la seguridad pública y su prevención, de tal forma que el tratamiento de datos personales para estos otros fines, en la medida en que esté incluido en el ámbito del Derecho de la Unión, entra en el ámbito de aplicación del presente Reglamento.

En lo que respecta al tratamiento de datos personales por parte de dichas autoridades competentes con fines que entren en el ámbito de aplicación del presente Reglamento, los Estados miembros deben tener la posibilidad de mantener o introducir disposiciones más específicas para adaptar la aplicación de las normas del presente Reglamento. Tales disposiciones pueden establecer de forma más precisa requisitos concretos para el tratamiento de datos personales con otros fines por parte de dichas autoridades competentes, tomando en consideración la estructura constitucional, organizativa y administrativa del Estado miembro en cuestión. Cuando el tratamiento de datos personales por organismos privados entre en el ámbito de aplicación del presente Reglamento, este debe disponer que los Estados miembros puedan, en condiciones específicas, limitar conforme a Derecho determinadas obligaciones y derechos siempre que dicha limitación sea una medida necesaria y proporcionada en una sociedad democrática para proteger intereses específicos importantes, entre ellos la seguridad pública y la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, inclusive la protección frente a las amenazas contra la seguridad pública y su prevención. Esto se aplica, por ejemplo, en el marco de la lucha contra el blanqueo de capitales o de las actividades de los laboratorios de policía científica.

(20) Aunque el presente Reglamento se aplica, entre otras, a las actividades de los tribunales y otras autoridades judiciales, en virtud del Derecho de la Unión o de los Estados

miembros pueden especificarse las operaciones de tratamiento y los procedimientos de tratamiento en relación con el tratamiento de datos personales por los tribunales y otras autoridades judiciales. A fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial. El control de esas operaciones de tratamiento de datos ha de poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular, garantizar el cumplimiento de las normas del presente Reglamento, concienciar más a los miembros del poder judicial acerca de sus obligaciones en virtud de este y atender las reclamaciones en relación con tales operaciones de tratamiento de datos.

(21) El presente Reglamento debe entenderse sin perjuicio de la aplicación de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo [8], en particular de las normas en materia de responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15. El objetivo de dicha Directiva es contribuir al correcto funcionamiento del mercado interior garantizando la libre circulación de los servicios de la sociedad de la información entre los Estados miembros.

(22) Todo tratamiento de datos personales en el contexto de las actividades de un establecimiento de un responsable o un encargado del tratamiento en la Unión debe llevarse a cabo de conformidad con el presente Reglamento, independientemente de que el tratamiento tenga lugar en la Unión. Un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto.

(23) Con el fin de garantizar que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud del presente Reglamento, el tratamiento de datos personales de interesados que se encuentran en la Unión por un responsable o un encargado no establecido en la Unión debe regirse por el presente Reglamento si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados, independientemente de que medie pago. Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que se encuentran en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.

(24) El tratamiento de datos personales de los interesados que se encuentran en la Unión por un responsable o encargado no establecido en la Unión debe ser también objeto del presente Reglamento cuando esté relacionado con la observación del comportamiento de dichos interesados en la medida en que este comportamiento tenga lugar en la Unión. Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

(25) Cuando sea de aplicación el Derecho de los Estados miembros en virtud del Derecho internacional público, el presente Reglamento debe aplicarse también a todo responsable del tratamiento no establecido en la Unión, como en una misión diplomática u oficina consular de un Estado miembro.

(26) Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de

información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

(27) El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas.

(28) La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.

(29) Para incentivar la aplicación de la seudonimización en el tratamiento de datos personales, debe ser posible establecer medidas de seudonimización, permitiendo al mismo tiempo un análisis general, por parte del mismo responsable del tratamiento, cuando este haya adoptado las medidas técnicas y organizativas necesarias para garantizar que se aplique el presente Reglamento al tratamiento correspondiente y que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concreta. El responsable que trate datos personales debe indicar cuáles son sus personas autorizadas.

(30) Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas.

(31) Las autoridades públicas a las que se comunican datos personales en virtud de una obligación legal para el ejercicio de su misión oficial, como las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores, no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros. Las solicitudes de comunicación de las autoridades públicas siempre deben presentarse por escrito, de forma motivada y con carácter ocasional, y no deben referirse a la totalidad de un fichero ni dar lugar a la interconexión de varios ficheros. El tratamiento de datos personales por dichas autoridades públicas debe ser conforme con la normativa en materia de protección de datos que sea de aplicación en función de la finalidad del tratamiento.

(32) El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las

actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

(33) Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida.

(34) Debe entenderse por datos genéticos los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente.

(35) Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo [(9)]; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

(36) El establecimiento principal de un responsable del tratamiento en la Unión debe ser el lugar de su administración central en la Unión, salvo que las decisiones relativas a los fines y medios del tratamiento de los datos personales se tomen en otro establecimiento del responsable en la Unión, en cuyo caso, ese otro establecimiento debe considerarse el establecimiento principal. El establecimiento principal de un responsable en la Unión debe determinarse en función de criterios objetivos y debe implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento a través de modalidades estables. Dicho criterio no debe depender de si el tratamiento de los datos personales se realiza en dicho lugar. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituyen, en sí mismas, establecimiento principal y no son, por lo tanto, criterios determinantes de un establecimiento principal. El establecimiento principal del encargado del tratamiento debe ser el lugar de su administración central en la Unión o, si careciese de administración central en la Unión, el lugar en el que se llevan a cabo las principales actividades de tratamiento en la Unión. En los casos que impliquen tanto al responsable como al encargado, la autoridad de control principal competente debe seguir siendo la autoridad de control del Estado miembro en el que el responsable tenga su establecimiento principal, pero la autoridad de control del encargado debe considerarse autoridad de control interesada y participar en el procedimiento de cooperación establecido en el presente Reglamento. En cualquier caso, las autoridades de control del Estado miembro o los Estados miembros en los que el encargado tenga uno o varios establecimientos no deben considerarse autoridades de control interesadas cuando el proyecto de decisión afecte únicamente al responsable. Cuando el tratamiento lo realice un grupo empresarial, el establecimiento principal de la empresa que ejerce el control debe considerarse el establecimiento principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine otra empresa.

(37) Un grupo empresarial debe estar constituido por una empresa que ejerce el control y las empresas controladas, debiendo ser la empresa que ejerce el control la que pueda ejercer una influencia dominante en las otras empresas, por razones, por ejemplo, de propiedad, participación financiera, normas por las que se rige, o poder de hacer cumplir las normas de protección de datos personales. Una empresa que controle el tratamiento de los datos personales en las empresas que estén afiliadas debe considerarse, junto con dichas empresas, «grupo empresarial».

(38) Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños.

(39) Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

(40) Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato.

(41) Cuando el presente Reglamento hace referencia a una base jurídica o a una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento, sin perjuicio de los requisitos de conformidad del ordenamiento constitucional del Estado miembro de que se trate. Sin embargo, dicha base jurídica o medida legislativa debe ser clara y precisa y su aplicación previsible para sus destinatarios, de conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, «Tribunal de Justicia») y del Tribunal Europeo de Derechos Humanos.

(42) Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En particular en el contexto de una declaración

por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. De acuerdo con la Directiva 93/13/CEE del Consejo [10], debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

(43) Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento.

(44) El tratamiento debe ser lícito cuando sea necesario en el contexto de un contrato o de la intención de concluir un contrato.

(45) Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros. El presente Reglamento no requiere que cada tratamiento individual se rija por una norma específica. Una norma puede ser suficiente como base para varias operaciones de tratamiento de datos basadas en una obligación legal aplicable al responsable del tratamiento, o si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. La finalidad del tratamiento también debe determinase en virtud del Derecho de la Unión o de los Estados miembros. Además, dicha norma podría especificar las condiciones generales del presente Reglamento por las que se rige la licitud del tratamiento de datos personales, establecer especificaciones para la determinación del responsable del tratamiento, el tipo de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y leal. Debe determinarse también en virtud del Derecho de la Unión o de los Estados miembros si el responsable del tratamiento que realiza una misión en interés público o en el ejercicio de poderes públicos debe ser una autoridad pública u otra persona física o jurídica de Derecho público, o, cuando se haga en interés público, incluidos fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad, de Derecho privado, como una asociación profesional.

(46) El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

(47) El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo,

cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo.

(48) Los responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados. Los principios generales aplicables a la transmisión de datos personales, dentro de un grupo empresarial, a una empresa situada en un país tercero no se ven afectados.

(49) Constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.

(50) El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros. Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior. Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.

Si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines. En todo caso, se debe garantizar la aplicación de los principios establecidos por el presente Reglamento y, en particular, la información del interesado sobre esos otros fines y sobre sus derechos, incluido el derecho de oposición. La indicación de posibles actos delictivos o amenazas para la seguridad pública por parte del responsable del tratamiento y la transmisión a la autoridad competente de los datos respecto de casos individuales o casos diversos relacionados con un mismo acto delictivo o amenaza para la seguridad pública debe considerarse que es en interés legítimo del responsable. Con todo, debe prohibirse esa transmisión en interés legítimo del responsable o el tratamiento ulterior de datos personales si el tratamiento no es compatible con una obligación de secreto legal, profesional o vinculante por otro concepto.

(51) Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas. El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.

(52) Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial.

(53) Las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para

lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, en particular en el contexto de la gestión de los servicios y sistemas sanitarios o de protección social, incluido el tratamiento de esos datos por las autoridades gestoras de la sanidad y las autoridades sanitarias nacionales centrales con fines de control de calidad, gestión de la información y supervisión general nacional y local del sistema sanitario o de protección social, y garantía de la continuidad de la asistencia sanitaria o la protección social y la asistencia sanitaria transfronteriza o fines de seguridad, supervisión y alerta sanitaria, o con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, basados en el Derecho de la Unión o del Estado miembro que ha de cumplir un objetivo de interés público, así como para estudios realizados en interés público en el ámbito de la salud pública. Por tanto, el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud, en relación con necesidades específicas, en particular si el tratamiento de esos datos lo realizan, con fines relacionados con la salud, personas sujetas a la obligación legal de secreto profesional. El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas. Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos.

(54) El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo [(11)], es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines.

(55) Se realiza además por razones de interés público el tratamiento de datos personales por las autoridades públicas con el fin de alcanzar los objetivos, establecidos en el Derecho constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente.

(56) Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas.

(57) Si los datos personales tratados por un responsable no le permiten identificar a una persona física, el responsable no debe estar obligado a obtener información adicional para identificar al interesado con la única finalidad de cumplir cualquier disposición del presente Reglamento. No obstante, el responsable del tratamiento no debe negarse a recibir información adicional facilitada por el interesado a fin de respaldarle en el ejercicio de sus derechos. La identificación debe incluir la identificación digital de un interesado, por ejemplo mediante un mecanismo de autenticación, como las mismas credenciales, empleadas por el interesado para abrir una sesión en el servicio en línea ofrecido por el responsable.

(58) El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le

conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender.

(59) Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos. El responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas.

(60) Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. Se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran. Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente.

(61) Se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso. Si los datos personales pueden ser comunicados legítimamente a otro destinatario, se debe informar al interesado en el momento en que se comunican al destinatario por primera vez. El responsable del tratamiento que proyecte tratar los datos para un fin que no sea aquel para el que se recogieron debe proporcionar al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y otra información necesaria. Cuando el origen de los datos personales no pueda facilitarse al interesado por haberse utilizado varias fuentes, debe facilitarse información general.

(62) Sin embargo, no es necesario imponer la obligación de proporcionar información cuando el interesado ya posea la información, cuando el registro o la comunicación de los datos personales estén expresamente establecidos por ley, o cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado. Tal podría ser particularmente el caso cuando el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas.

(63) Los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Ello incluye el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas. Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento. Si es posible, el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales. Este derecho no debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos. No obstante, estas consideraciones no deben tener

como resultado la negativa a prestar toda la información al interesado. Si trata una gran cantidad de información relativa al interesado, el responsable del tratamiento debe estar facultado para solicitar que, antes de facilitarse la información, el interesado especifique la información o actividades de tratamiento a que se refiere la solicitud.

(64) El responsable del tratamiento debe utilizar todas las medidas razonables para verificar la identidad de los interesados que soliciten acceso, en particular en el contexto de los servicios en línea y los identificadores en línea. El responsable no debe conservar datos personales con el único propósito de poder responder a posibles solicitudes.

(65) Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un «derecho al olvido» si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

(66) A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.

(67) Entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema.

(68) Para reforzar aún más el control sobre sus propios datos, cuando el tratamiento de los datos personales se efectúe por medios automatizados, debe permitirse asimismo que los interesados que hubieran facilitado datos personales que les conciernan a un responsable del tratamiento los reciban en un formato estructurado, de uso común, de lectura mecánica e interoperable, y los transmitan a otro responsable del tratamiento. Debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de datos. Dicho derecho debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato. No debe aplicarse cuando el tratamiento tiene una base jurídica distinta del consentimiento o el contrato. Por su propia naturaleza, dicho derecho no debe ejercerse en contra de responsables que traten datos personales en el ejercicio de sus funciones públicas. Por lo tanto, no debe aplicarse, cuando el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al

responsable. El derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles. Cuando un conjunto de datos personales determinado concierna a más de un interesado, el derecho a recibir tales datos se debe entender sin menoscabo de los derechos y libertades de otros interesados de conformidad con el presente Reglamento. Por otra parte, ese derecho no debe menoscabar el derecho del interesado a obtener la supresión de los datos personales y las limitaciones de ese derecho recogidas en el presente Reglamento, y en particular no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato. El interesado debe tener derecho a que los datos personales se transmitan directamente de un responsable del tratamiento a otro, cuando sea técnicamente posible.

(69) En los casos en que los datos personales puedan ser tratados lícitamente porque el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o por motivos de intereses legítimos del responsable o de un tercero, el interesado debe, sin embargo, tener derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular. Debe ser el responsable el que demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado.

(70) Si los datos personales son tratados con fines de mercadotecnia directa, el interesado debe tener derecho a oponerse a dicho tratamiento, inclusive a la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia directa, ya sea con respecto a un tratamiento inicial o ulterior, y ello en cualquier momento y sin coste alguno. Dicho derecho debe comunicarse explícitamente al interesado y presentarse claramente y al margen de cualquier otra información.

(71) El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar, como la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna. Este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Sin embargo, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión. Tal medida no debe afectar a un menor.

A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para

los intereses y derechos del interesado e impedir, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o tratamiento que dé lugar a medidas que produzcan tal efecto. Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas.

(72) La elaboración de perfiles está sujeta a las normas del presente Reglamento que rigen el tratamiento de datos personales, como los fundamentos jurídicos del tratamiento o los principios de la protección de datos. El Comité Europeo de Protección de Datos establecido por el presente Reglamento (en lo sucesivo, el «Comité») debe tener la posibilidad de formular orientaciones en este contexto.

(73) El Derecho de la Unión o de los Estados miembros puede imponer restricciones a determinados principios y a los derechos de información, acceso, rectificación o supresión de datos personales, al derecho a la portabilidad de los datos, al derecho de oposición, a las decisiones basadas en la elaboración de perfiles, así como a la comunicación de una violación de la seguridad de los datos personales a un interesado y a determinadas obligaciones conexas de los responsables del tratamiento, en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano, la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública o de violaciones de normas deontológicas en las profesiones reguladas, y su prevención, otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un importante interés económico o financiero de la Unión o de un Estado miembro, la llevanza de registros públicos por razones de interés público general, el tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios, o la protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios. Dichas restricciones deben ajustarse a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

(74) Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas.

(75) Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

(76) La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

(77) Se podrían proporcionar directrices para la aplicación de medidas oportunas y para demostrar el cumplimiento por parte del responsable o del encargado del tratamiento, especialmente con respecto a la identificación del riesgo relacionado con el tratamiento, a su evaluación en términos de origen, naturaleza, probabilidad y gravedad y a la identificación de buenas prácticas para mitigar el riesgo, que revistan, en particular, la forma de códigos de conducta aprobados, certificaciones aprobadas, directrices dadas por el Comité o indicaciones proporcionadas por un delegado de protección de datos. El Comité también puede emitir directrices sobre operaciones de tratamiento que se considere improbable supongan un alto riesgo para los derechos y libertades de las personas físicas, e indicar qué medidas pueden ser suficientes en dichos casos para afrontar el riesgo en cuestión.

(78) La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

(79) La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, requieren una atribución clara de las responsabilidades en virtud del presente Reglamento, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable.

(80) El responsable o el encargado del tratamiento no establecido en la Unión que esté tratando datos personales de interesados que se encuentran en la Unión y cuyas actividades de tratamiento están relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si se requiere un pago por parte de estos, o con el control de su comportamiento en la medida en que este tenga lugar en la Unión, debe designar a un representante, a menos que el tratamiento sea ocasional, no incluya el tratamiento a gran escala de categorías especiales de datos personales o el tratamiento de datos personales relativos a condenas e infracciones penales, y sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, vista la naturaleza, el contexto, el ámbito y los fines del tratamiento, o si el responsable del tratamiento es una autoridad u organismo público. El representante debe actuar por cuenta del responsable o el encargado y puede ser contactado por cualquier autoridad de control. El representante debe ser designado expresamente por mandato escrito del responsable o del encargado para que actúe en su nombre con respecto a las obligaciones que les incumben en virtud del presente Reglamento. La designación de dicho representante no afecta a la responsabilidad del responsable o del encargado en virtud del presente Reglamento. Dicho representante debe

desempeñar sus funciones conforme al mandato recibido del responsable o del encargado, incluida la cooperación con las autoridades de control competentes en relación con cualquier medida que se tome para garantizar el cumplimiento del presente Reglamento. El representante designado debe estar sujeto a medidas coercitivas en caso de incumplimiento por parte del responsable o del encargado.

(81) Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable. El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado. El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión. Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos.

(82) Para demostrar la conformidad con el presente Reglamento, el responsable o el encargado del tratamiento debe mantener registros de las actividades de tratamiento bajo su responsabilidad. Todos los responsables y encargados están obligados a cooperar con la autoridad de control y a poner a su disposición, previa solicitud, dichos registros, de modo que puedan servir para supervisar las operaciones de tratamiento.

(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

(84) A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento.

(85) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de

sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

(86) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

(87) Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento.

(88) Al establecer disposiciones de aplicación sobre el formato y los procedimientos aplicables a la notificación de las violaciones de la seguridad de los datos personales, hay que tener debidamente en cuenta las circunstancias de tal violación, inclusive si los datos personales habían sido protegidos mediante las medidas técnicas de protección adecuadas, limitando eficazmente la probabilidad de usurpación de identidad u otras formas de uso indebido. Asimismo, estas normas y procedimientos deben tener en cuenta los intereses legítimos de las autoridades policiales en caso de que una comunicación prematura pueda obstaculizar innecesariamente la investigación de las circunstancias de una violación de la seguridad de los datos personales.

(89) La Directiva 95/46/CE estableció la obligación general de notificar el tratamiento de datos personales a las autoridades de control. Pese a implicar cargas administrativas y financieras, dicha obligación, sin embargo, no contribuyó en todos los casos a mejorar la protección de los datos personales. Por tanto, estas obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas. Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial.

(90) En tales casos, el responsable debe llevar a cabo, antes del tratamiento, una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular

gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento.

(91) Lo anterior debe aplicarse, en particular, a las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala y a otras operaciones de tratamiento que entrañan un alto riesgo para los derechos y libertades de los interesados, en particular cuando estas operaciones hace más difícil para los interesados el ejercicio de sus derechos. La evaluación de impacto relativa a la protección de datos debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas. También es necesaria una evaluación de impacto relativa a la protección de datos para el control de zonas de acceso público a gran escala, en particular cuando se utilicen dispositivos optoelectrónicos o para cualquier otro tipo de operación cuando la autoridad de control competente considere que el tratamiento entrañe probablemente un alto riesgo para los derechos y libertades de los interesados, en particular porque impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato, o porque se efectúe sistemáticamente a gran escala. El tratamiento de datos personales no debe considerarse a gran escala si lo realiza, respecto de datos personales de pacientes o clientes, un solo médico, otro profesional de la salud o abogado. En estos casos, la evaluación de impacto de la protección de datos no debe ser obligatoria.

(92) Hay circunstancias en las que puede ser razonable y económico que una evaluación de impacto relativa a la protección de datos abarque más de un único proyecto, por ejemplo, en el caso de que las autoridades u organismos públicos prevean crear una aplicación o plataforma común de tratamiento, o si varios responsables proyecten introducir una aplicación o un entorno de tratamiento común en un sector o segmento empresarial o para una actividad horizontal de uso generalizado.

(93) Los Estados miembros, al adoptar el Derecho en el que se basa el desempeño de las funciones de la autoridad pública o el organismo público y que regula la operación o el conjunto de operaciones de tratamiento en cuestión, pueden considerar necesario llevar a cabo dicha evaluación con carácter previo a las actividades de tratamiento.

(94) Debe consultarse a la autoridad de control antes de iniciar las actividades de tratamiento si una evaluación de impacto relativa a la protección de datos muestra que, en ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos, el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas, y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación. Existe la probabilidad de que ese alto riesgo se deba a determinados tipos de tratamiento y al alcance y frecuencia de este, lo que también puede ocasionar daños y perjuicios o una injerencia en los derechos y libertades de la persona física. La autoridad de control debe responder a la solicitud de consulta dentro de un plazo determinado. Sin embargo, la ausencia de respuesta de la autoridad de control dentro de dicho plazo no debe obstar a cualquier intervención de dicha autoridad basada en las funciones y poderes que le atribuye el presente Reglamento, incluido el poder de prohibir operaciones de tratamiento. Como parte de dicho proceso de consulta, se puede presentar a la autoridad de control el resultado de una evaluación de impacto relativa a la protección de datos efectuada en relación con el tratamiento en cuestión, en particular las medidas previstas para mitigar los riesgos para los derechos y libertades de las personas físicas.

(95) El encargado del tratamiento debe asistir al responsable cuando sea necesario y a petición suya, a fin de asegurar que se cumplen las obligaciones que se derivan de la

realización de las evaluaciones de impacto relativas a la protección de datos y de la consulta previa a la autoridad de control.

(96) Deben llevarse también a cabo consultas con la autoridad de control en el curso de la tramitación de una medida legislativa o reglamentaria que establezca el tratamiento de datos personales, a fin de garantizar la conformidad del tratamiento previsto con el presente Reglamento y, en particular, de mitigar el riesgo que implique el tratamiento para el interesado.

(97) Al supervisar la observancia interna del presente Reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial, si el tratamiento lo realiza en el sector privado un responsable cuyas actividades principales consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados, o si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales. En el sector privado, las actividades principales de un responsable están relacionadas con sus actividades primarias y no están relacionadas con el tratamiento de datos personales como actividades auxiliares. El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente.

(98) Se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. Dichos códigos de conducta podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento.

(99) Al elaborar un código de conducta, o al modificar o ampliar dicho código, las asociaciones y otros organismos que representan a categorías de responsables o encargados deben consultar a las partes interesadas, incluidos los interesados cuando sea posible, y tener en cuenta las consideraciones transmitidas y las opiniones manifestadas en respuesta a dichas consultas.

(100) A fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes.

(101) Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales. El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. No obstante, si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión por el presente Reglamento, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional. En todo caso, las transferencias a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el presente Reglamento. Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales.

(102) El presente Reglamento se entiende sin perjuicio de los acuerdos internacionales celebrados entre la Unión y terceros países que regulan la transferencia de datos personales, incluidas las oportunas garantías para los interesados. Los Estados miembros pueden celebrar acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales siempre que dichos acuerdos no afecten al presente Reglamento ni a ninguna otra disposición del Derecho de la Unión e incluyan un nivel adecuado de protección de los derechos fundamentales de los interesados.

(103) La Comisión puede decidir, con efectos para toda la Unión, que un tercer país, un territorio o un sector específico de un tercer país, o una organización internacional ofrece un nivel de protección de datos adecuado, aportando de esta forma en toda la Unión seguridad y uniformidad jurídicas en lo que se refiere al tercer país u organización internacional que se considera ofrece tal nivel de protección. En estos casos, se pueden realizar transferencias de datos personales a estos países sin que se requiera obtener otro tipo de autorización. La Comisión también puede decidir revocar esa decisión, previo aviso y completa declaración motivada al tercer país u organización internacional.

(104) En consonancia con los valores fundamentales en los que se basa la Unión, en particular la protección de los derechos humanos, la Comisión, en su evaluación del tercer país, o de un territorio o un sector específico de un tercer país, debe tener en cuenta de qué manera respeta un determinado tercer país respeta el Estado de Derecho, el acceso a la justicia y las normas y criterios internacionales en materia de derechos humanos y su Derecho general y sectorial, incluida la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el orden público y el Derecho penal. En la adopción de una decisión de adecuación con respecto a un territorio o un sector específico de un tercer país se deben tener en cuenta criterios claros y objetivos, como las actividades concretas de tratamiento y el alcance de las normas jurídicas aplicables y la legislación vigente en el tercer país. El tercer país debe ofrecer garantías que aseguren un nivel adecuado de protección equivalente en lo esencial al ofrecido en la Unión, en particular cuando los datos personales son objeto de tratamiento en uno o varios sectores específicos. En particular, el tercer país debe garantizar que haya un control verdaderamente independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros, así como reconocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas.

(105) Aparte de los compromisos internacionales adquiridos por el tercer país u organización internacional, la Comisión debe tener en cuenta las obligaciones resultantes de la participación del tercer país u organización internacional en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales, y el cumplimiento de esas obligaciones. En particular, debe tenerse en cuenta la adhesión del país al Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo adicional. La Comisión debe consultar al Comité al evaluar el nivel de protección existente en terceros países u organizaciones internacionales.

(106) La Comisión debe supervisar la aplicación de las decisiones sobre el nivel de protección en un país tercero, un territorio o un sector específico de un país tercero, o una organización internacional, y la aplicación las decisiones adoptadas sobre la base del artículo 25, apartado 6, o el artículo 26, apartado 4, de la Directiva 95/46/CE. En sus decisiones de adecuación, la Comisión debe establecer un mecanismo para la revisión periódica de su aplicación. Dicha revisión periódica debe realizarse en colaboración con el tercer país u organización internacional de que se trate y tener en cuenta todos los cambios en la materia que se produzcan en dicho tercer país u organización internacional. A efectos de la supervisión y realización de las revisiones periódicas, la Comisión debe tomar en consideración las opiniones y conclusiones del Parlamento Europeo y del Consejo, así como de otros organismos y fuentes pertinentes. La Comisión debe evaluar, en un plazo razonable, la aplicación de dichas decisiones e informar de cualquier conclusión pertinente al Comité que, en el sentido del Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo [(12)], establece el presente Reglamento, y al Parlamento Europeo y el Consejo.

(107) La Comisión puede reconocer que un tercer país, un territorio o sector específico en un tercer país, o una organización internacional ya no garantiza un nivel de protección de

datos adecuado. En consecuencia, debe prohibirse la transferencia de datos personales a dicho tercer país u organización internacional, salvo que se cumplan los requisitos del presente Reglamento relativos a las transferencias basadas en garantías adecuadas, incluidas las normas corporativas vinculantes, y a las excepciones aplicadas a situaciones específicas. En ese caso, debe establecerse la celebración de consultas entre la Comisión y esos terceros países u organizaciones internacionales. La Comisión debe informar en tiempo oportuno al tercer país u organización internacional de las razones y entablar consultas a fin de subsanar la situación.

(108) En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado. Tales garantías adecuadas pueden consistir en el recurso a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, incluida la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto. Las transferencias también pueden realizarlas autoridades o entidades públicas con entidades o autoridades públicas de terceros países o con organizaciones internacionales con competencias o funciones correspondientes, igualmente sobre la base de disposiciones incorporadas a acuerdos administrativos, como un memorando de entendimiento, que reconozcan derechos exigibles y efectivos a los interesados. Si las garantías figuran en acuerdos administrativos que no sean jurídicamente vinculantes se debe recabar la autorización de la autoridad de control competente.

(109) La posibilidad de que el responsable o el encargado del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión o una autoridad de control no debe obstar a que los responsables o encargados incluyan las cláusulas tipo de protección de datos en un contrato más amplio, como un contrato entre dos encargados, o a que añadan otras cláusulas o garantías adicionales, siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo adoptadas por la Comisión o por una autoridad de control, ni mermen los derechos o las libertades fundamentales de los interesados. Se debe alentar a los responsables y encargados del tratamiento a ofrecer garantías adicionales mediante compromisos contractuales que complementen las cláusulas tipo de protección de datos.

(110) Todo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta debe tener la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales de la Unión a organizaciones dentro del mismo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta, siempre que tales normas corporativas incorporen todos los principios esenciales y derechos aplicables con el fin de ofrecer garantías adecuadas para las transferencias o categorías de transferencias de datos de carácter personal.

(111) Se debe establecer la posibilidad de realizar transferencias en determinadas circunstancias, de mediar el consentimiento explícito del interesado, si la transferencia es ocasional y necesaria en relación con un contrato o una reclamación, independientemente de tratarse de un procedimiento judicial o un procedimiento administrativo o extrajudicial, incluidos los procedimientos ante organismos reguladores. También se debe establecer la posibilidad de realizar transferencias cuando así lo requieran razones importantes de interés público establecidas por el Derecho de la Unión o de los Estados miembros, o cuando la transferencia se haga a partir de un registro establecido por ley y se destine a consulta por el público o por personas que tengan un interés legítimo. En este último caso la transferencia no debe afectar a la totalidad de los datos personales o de las categorías de datos incluidos en el registro y, cuando el registro esté destinado a su consulta por personas que tengan un interés legítimo, la transferencia solo debe efectuarse a petición de dichas personas o, si

estas van a ser las destinatarias, teniendo plenamente en cuenta los intereses y los derechos fundamentales del interesado.

(112) Dichas excepciones deben aplicarse en particular a las transferencias de datos requeridas y necesarias por razones importantes de interés público, por ejemplo en caso de intercambios internacionales de datos entre autoridades en el ámbito de la competencia, administraciones fiscales o aduaneras, entre autoridades de supervisión financiera, entre servicios competentes en materia de seguridad social o de sanidad pública, por ejemplo en caso contactos destinados a localizar enfermedades contagiosas o para reducir y/o eliminar el dopaje en el deporte. La transferencia de datos personales también debe considerarse lícita en caso de que sea necesaria para proteger un interés esencial para los intereses vitales del interesado o de otra persona, incluida la integridad física o la vida, si el interesado no está en condiciones de dar su consentimiento. En ausencia de una decisión de adecuación, el Derecho de la Unión o de los Estados miembros puede limitar expresamente, por razones importantes de interés público, la transferencia de categorías específicas de datos a un tercer país o a una organización internacional. Los Estados miembros deben notificar esas disposiciones a la Comisión. Puede considerarse necesaria, por una razón importante de interés público o por ser de interés vital para el interesado, toda transferencia a una organización internacional humanitaria de datos personales de un interesado que no tenga capacidad física o jurídica para dar su consentimiento, con el fin de desempeñar un cometido basado en las Convenciones de Ginebra o de conformarse al Derecho internacional humanitario aplicable en caso de conflictos armados.

(113) Las transferencias que pueden calificarse de no repetitivas y sólo se refieren a un número limitado de interesados, también han de ser posibles en caso de servir a intereses legítimos imperiosos del responsable del tratamiento, si no prevalecen sobre ellos los intereses o los derechos y libertades del interesado y el responsable ha evaluado todas las circunstancias concurrentes en la transferencia de datos. El responsable debe prestar especial atención a la naturaleza de los datos personales, la finalidad y la duración de la operación o las operaciones de tratamiento propuestas, así como la situación en el país de origen, el tercer país y el país de destino final, y ofrecer, garantías apropiadas para proteger los derechos fundamentales y las libertades de las personas físicas con respecto al tratamiento de sus datos personales. Dichas transferencias sólo deben ser posibles en casos aislados, cuando ninguno de los otros motivos para la transferencia sean aplicables. Las legítimas expectativas de la sociedad en un aumento del conocimiento se deben tener en cuenta para fines de investigación científica o histórica o fines estadísticos. El responsable debe informar de la transferencia a la autoridad de control y al interesado.

(114) En cualquier caso, cuando la Comisión no haya tomado ninguna decisión sobre el nivel adecuado de la protección de datos en un tercer país, el responsable o el encargado del tratamiento deben arbitrar soluciones que garanticen a los interesados derechos exigibles y efectivos con respecto al tratamiento de sus datos en la Unión, una vez transferidos estos, de forma que sigan beneficiándose de derechos fundamentales y garantías.

(115) Algunos países terceros adoptan leyes, reglamentaciones y otros actos jurídicos con los que se pretende regular directamente las actividades de tratamiento de personas físicas y jurídicas bajo jurisdicción de los Estados miembros. Esto puede incluir sentencias de órganos jurisdiccionales o decisiones de autoridades administrativas de terceros países que obliguen a un responsable o un encargado del tratamiento a transferir o comunicar datos personales, y que no se basen en un acuerdo internacional, como un tratado de asistencia judicial mutua, en vigor entre el tercer país requirente y la Unión o un Estado miembro. La aplicación extraterritorial de dichas leyes, reglamentaciones y otros actos jurídicos puede ser contraria al Derecho internacional e impedir la protección de las personas físicas garantizada en la Unión en virtud del presente Reglamento. Las transferencias solo deben autorizarse cuando se cumplan las condiciones del presente Reglamento relativas a las transferencias a terceros países. Tal puede ser el caso, entre otros, cuando la comunicación sea necesaria por una razón importante de interés público reconocida por el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento.

(116) Cuando los datos personales circulan a través de las fronteras hacia el exterior de la Unión se puede poner en mayor riesgo la capacidad de las personas físicas para ejercer

los derechos de protección de datos, en particular con el fin de protegerse contra la utilización o comunicación ilícitas de dicha información. Al mismo tiempo, es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades desarrolladas fuera de sus fronteras. Sus esfuerzos por colaborar en el contexto transfronterizo también pueden verse obstaculizados por poderes preventivos o correctivos insuficientes, regímenes jurídicos incoherentes y obstáculos prácticos, como la escasez de recursos. Por consiguiente, es necesario fomentar una cooperación más estrecha entre las autoridades de control encargadas de la protección de datos para ayudarlas a intercambiar información y a llevar a cabo investigaciones con sus homólogos internacionales. A fin de desarrollar mecanismos de cooperación internacional que faciliten y proporcionen asistencia internacional mutua en la ejecución de legislación en materia de protección de datos personales, la Comisión y las autoridades de control deben intercambiar información y cooperar en actividades relativas al ejercicio de sus competencias con las autoridades competentes de terceros países, sobre la base de la reciprocidad y de conformidad con el presente Reglamento.

(117) El establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa.

(118) La independencia de las autoridades de control no debe significar que dichas autoridades puedan quedar exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial.

(119) Si un Estado miembro establece varias autoridades de control, debe disponer por ley mecanismos que garanticen la participación efectiva de dichas autoridades de control en el mecanismo de coherencia. Tal Estado miembro debe, en particular, designar a la autoridad de control que actuará como punto de contacto único de cara a la participación efectiva de dichas autoridades en el citado mecanismo, garantizando así una cooperación rápida y fluida con otras autoridades de control, el Comité y la Comisión.

(120) Todas las autoridades de control deben estar dotadas de los recursos financieros y humanos, los locales y las infraestructuras que sean necesarios para la realización eficaz de sus funciones, en particular las relacionadas con la asistencia recíproca y la cooperación con otras autoridades de control de la Unión. Cada autoridad de control debe disponer de un presupuesto anual público propio, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

(121) Las condiciones generales aplicables al miembro o los miembros de la autoridad de control deben establecerse por ley en cada Estado miembro y disponer, en particular, que dichos miembros han de ser nombrados, por un procedimiento transparente, por el Parlamento, el Gobierno o el jefe de Estado del Estado miembro, a propuesta del Gobierno, de un miembro del Gobierno o del Parlamento o una de sus cámaras, o por un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros. A fin de garantizar la independencia de la autoridad de control, sus miembros deben actuar con integridad, abstenerse de cualquier acción que sea incompatible con sus funciones y no participar, mientras dure su mandato, en ninguna actividad profesional incompatible, sea o no remunerada. La autoridad de control debe tener su propio personal, seleccionado por esta o por un organismo independiente establecido por el Derecho de los Estados miembros, que esté subordinado exclusivamente al miembro o los miembros de la autoridad de control.

(122) Cada autoridad de control debe ser competente, en el territorio de su Estado miembro, para ejercer los poderes y desempeñar las funciones que se le confieran de conformidad con el presente Reglamento. Lo anterior debe abarcar, en particular, el tratamiento en el contexto de las actividades de un establecimiento del responsable o del encargado en el territorio de su Estado miembro, el tratamiento de datos personales realizado por autoridades públicas o por organismos privados que actúen en interés público, el tratamiento que afecte a interesados en su territorio, o el tratamiento realizado por un responsable o un encargado que no esté establecido en la Unión cuando sus destinatarios sean interesados residentes en su territorio. Debe incluirse el examen de reclamaciones

presentadas por un interesado, la realización de investigaciones sobre la aplicación del presente Reglamento y el fomento de la sensibilización del público acerca de los riesgos, las normas, las garantías y los derechos en relación con el tratamiento de datos personales.

(123) A fin de proteger a las personas físicas con respecto al tratamiento de sus datos personales y de facilitar la libre circulación de los datos personales en el mercado interior, las autoridades de control deben supervisar la aplicación de las disposiciones adoptadas de conformidad con el presente Reglamento y contribuir a su aplicación coherente en toda la Unión. A tal efecto, las autoridades de control deben cooperar entre ellas y con la Comisión, sin necesidad de acuerdo alguno entre Estados miembros sobre la prestación de asistencia mutua ni sobre dicha cooperación.

(124) Si el tratamiento de datos personales se realiza en el contexto de las actividades de un establecimiento de un responsable o un encargado en la Unión y el responsable o el encargado está establecido en más de un Estado miembro, o si el tratamiento en el contexto de las actividades de un único establecimiento de un responsable o un encargado en la Unión afecta o es probable que afecte sustancialmente a interesados en más de un Estado miembro, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado debe actuar como autoridad principal. Dicha autoridad debe cooperar con las demás autoridades interesadas, ya sea porque el responsable o el encargado tenga un establecimiento en el territorio de su Estado miembro, porque afecte sustancialmente a interesados que residen en su territorio, o porque se haya presentado una reclamación ante ellas. Asimismo, cuando un interesado que no resida en ese Estado miembro haya presentado una reclamación, la autoridad de control ante la que se haya presentado esta también debe ser autoridad de control interesada. En el marco de sus funciones de formulación de directrices sobre cualquier cuestión relacionada con la aplicación del presente Reglamento, el Comité debe estar facultado para formular directrices, en particular sobre los criterios que han de tenerse en cuenta para determinar si el tratamiento en cuestión afecta sustancialmente a interesados de más de un Estado miembro y sobre lo que constituya una objeción pertinente y motivada.

(125) La autoridad principal debe ser competente para adoptar decisiones vinculantes relativas a las medidas de aplicación de los poderes conferidos con arreglo al presente Reglamento. En su calidad de autoridad principal, la autoridad de control debe implicar estrechamente y coordinar a las autoridades de control interesadas en el proceso de toma de decisiones. En los casos en los que la decisión consista en rechazar total o parcialmente la reclamación del interesado, esa decisión debe ser adoptada por la autoridad de control ante la que se haya presentado la reclamación.

(126) La decisión debe ser acordada conjuntamente por la autoridad de control principal y las autoridades de control interesadas y debe dirigirse al establecimiento principal o único del responsable o del encargado del tratamiento y ser vinculante para ambos. El responsable o el encargado deben tomar las medidas necesarias para garantizar el cumplimiento del presente Reglamento y la aplicación de la decisión notificada por la autoridad de control principal al establecimiento principal del responsable o del encargado en lo que se refiere a las actividades de tratamiento en la Unión.

(127) Cada autoridad de control que no actúa como autoridad principal debe ser competente para tratar asuntos locales en los que, si bien el responsable o el encargado del tratamiento está establecido en más de un Estado miembro, el objeto del tratamiento específico se refiere exclusivamente al tratamiento efectuado en un único Estado miembro y afecta exclusivamente a interesados de ese único Estado miembro, por ejemplo cuando el tratamiento tiene como objeto datos personales de empleados en el contexto específico de empleo de un Estado miembro. En tales casos, la autoridad de control debe informar sin dilación al respecto a la autoridad de control principal. Una vez informada, la autoridad de control principal debe decidir si tratará el asunto de acuerdo con la disposición aplicable a la cooperación entre la autoridad de control principal y otras autoridades de control interesadas («mecanismo de ventanilla única»), o si lo debe tratar localmente la autoridad de control que le haya informado. Al decidir si trata el asunto, la autoridad de control principal debe considerar si existe un establecimiento del responsable o del encargado en el Estado miembro de la autoridad de control que le haya informado, con el fin de garantizar la ejecución efectiva de la decisión respecto del responsable o encargado del tratamiento. Si la

autoridad de control principal decide tratar el asunto, se debe ofrecer a la autoridad de control informante la posibilidad de presentar un proyecto de decisión, que la autoridad de control principal ha de tener en cuenta en la mayor medida posible al preparar su proyecto de decisión al amparo del mecanismo de ventanilla única.

(128) Las normas sobre la autoridad de control principal y el mecanismo de ventanilla única no deben aplicarse cuando el tratamiento sea realizado por autoridades públicas u organismos privados en interés público. En tales casos, la única autoridad de control competente para ejercer los poderes conferidos con arreglo al presente Reglamento debe ser la autoridad de control del Estado miembro en el que estén establecidos la autoridad pública o el organismo privado.

(129) Para garantizar la supervisión y ejecución coherentes del presente Reglamento en toda la Unión, las autoridades de control deben tener en todos los Estados miembros las mismas funciones y poderes efectivos, incluidos poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos, especialmente en casos de reclamaciones de personas físicas, y sin perjuicio de las competencias de las autoridades encargadas de la persecución de los delitos con arreglo al Derecho de los Estados miembros para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y ejercitar acciones judiciales. Dichos poderes deben incluir también el poder de imponer una limitación temporal o definitiva al tratamiento, incluida su prohibición. Los Estados miembros pueden especificar otras funciones relacionadas con la protección de datos personales con arreglo al presente Reglamento. Los poderes de las autoridades de control deben ejercerse de conformidad con garantías procesales adecuadas establecidas en el Derecho de la Unión y los Estados miembros, de forma imparcial, equitativa y en un plazo razonable. En particular, toda medida debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento del presente Reglamento, teniendo en cuenta las circunstancias de cada caso concreto, respetar el derecho de todas las personas a ser oídas antes de que se adopte cualquier medida que las afecte negativamente y evitar costes superfluos y molestias excesivas para las personas afectadas. Los poderes de investigación en lo que se refiere al acceso a instalaciones deben ejercerse de conformidad con los requisitos específicos del Derecho procesal de los Estados miembros, como el de la autorización judicial previa. Toda medida jurídicamente vinculante de la autoridad de control debe constar por escrito, ser clara e inequívoca, indicar la autoridad de control que dictó la medida y la fecha en que se dictó, llevar la firma del director o de un miembro de la autoridad de control autorizado por este, especificar los motivos de la medida y mencionar el derecho a la tutela judicial efectiva. Esto no debe obstar a que se impongan requisitos adicionales con arreglo al Derecho procesal de los Estados miembros. La adopción de una decisión jurídicamente vinculante implica que puede ser objeto de control judicial en el Estado miembro de la autoridad de control que adoptó la decisión.

(130) Cuando la autoridad de control ante la cual se haya presentado la reclamación no sea la autoridad de control principal, esta última debe cooperar estrechamente con la primera con arreglo a las disposiciones sobre cooperación y coherencia establecidas en el presente Reglamento. En tales casos, la autoridad de control principal, al tomar medidas concebidas para producir efectos jurídicos, incluida la imposición de multas administrativas, debe tener en cuenta en la mayor medida posible la opinión de la autoridad de control ante la cual se haya presentado la reclamación y la cual debe seguir siendo competente para realizar cualquier investigación en el territorio de su propio Estado miembro en enlace con la autoridad de control competente.

(131) En casos en los que otra autoridad de control deba actuar como autoridad de control principal para las actividades de tratamiento del responsable o del encargado pero el objeto concreto de una reclamación o la posible infracción afecta únicamente a las actividades de tratamiento del responsable o del encargado en el Estado miembro en el que se haya presentado la reclamación o detectado la posible infracción y el asunto no afecta sustancialmente ni es probable que afecte sustancialmente a interesados de otros Estados miembros, la autoridad de control que reciba una reclamación o que detecte situaciones que conlleven posibles infracciones del presente Reglamento o reciba de otra manera información sobre estas debe tratar de llegar a un arreglo amistoso con el responsable del tratamiento y, si no prospera, ejercer todos sus poderes. En lo anterior se debe incluir el

tratamiento específico realizado en el territorio del Estado miembro de la autoridad de control o con respecto a interesados en el territorio de dicho Estado miembro; el tratamiento efectuado en el contexto de una oferta de bienes o servicios destinada específicamente a interesados en el territorio del Estado miembro de la autoridad de control; o el tratamiento que deba evaluarse teniendo en cuenta las obligaciones legales pertinentes en virtud del Derecho de los Estados miembros.

(132) Entre las actividades de sensibilización del público por parte de las autoridades de control deben incluirse medidas específicas dirigidas a los responsables y los encargados del tratamiento, incluidas las microempresas y las pequeñas y medianas empresas, así como las personas físicas, en particular en el contexto educativo.

(133) Las autoridades de control se deben ayudar una a otra en el desempeño de sus funciones y prestar asistencia mutua, con el fin de garantizar la aplicación y ejecución coherentes del presente Reglamento en el mercado interior. Una autoridad de control que solicite asistencia mutua puede adoptar una medida provisional si no recibe respuesta a su solicitud de asistencia en el plazo de un mes a partir de su recepción por la otra autoridad de control.

(134) Cada autoridad de control debe participar, cuando proceda, en operaciones conjuntas con otras autoridades de control. La autoridad de control a la que se solicite ayuda debe tener la obligación de responder a la solicitud en un plazo de tiempo determinado.

(135) A fin de garantizar la aplicación coherente del presente Reglamento en toda la Unión, debe establecerse un mecanismo de coherencia para la cooperación entre las autoridades de control. Este mecanismo debe aplicarse en particular cuando una autoridad de control prevea adoptar una medida dirigida a producir efectos jurídicos en lo que se refiere a operaciones de tratamiento que afecten sustancialmente a un número significativo de interesados en varios Estados miembros. También debe aplicarse cuando cualquier autoridad de control interesada o la Comisión soliciten que dicho asunto se trate al amparo del mecanismo de coherencia. Dicho mecanismo debe entenderse sin perjuicio de cualesquiera medidas que la Comisión pueda adoptar en el ejercicio de sus poderes con arreglo a los Tratados.

(136) En aplicación del mecanismo de coherencia, el Comité debe, en un plazo determinado, emitir un dictamen, si así lo decide una mayoría de sus miembros o si así lo solicita cualquier autoridad de control interesada o la Comisión. El Comité también debe estar facultado para adoptar decisiones jurídicamente vinculantes en caso de diferencias entre autoridades de control. A tal efecto debe dictar, en principio por mayoría de dos tercios de sus miembros, decisiones jurídicamente vinculantes en casos claramente especificados en los que exista conflicto de opiniones entre las autoridades de control, en particular en el mecanismo de cooperación entre la autoridad de control principal y las autoridades de control interesadas sobre el fondo del asunto, especialmente en caso de infracción del presente Reglamento.

(137) La necesidad urgente de actuar puede obedecer a la necesidad de proteger los derechos y libertades de los interesados, en particular cuando exista el riesgo de que pueda verse considerablemente obstaculizado el reconocimiento de alguno de sus derechos. Por lo tanto, una autoridad de control debe poder adoptar en su territorio medidas provisionales, debidamente justificadas, con un plazo de validez determinado no superior a tres meses.

(138) La aplicación de tal mecanismo debe ser una condición para la licitud de una medida de una autoridad de control destinada a producir efectos jurídicos, en aquellos casos en los que su aplicación sea obligatoria. En otros casos de relevancia transfronteriza, la autoridad de control principal y las autoridades de control interesadas deben aplicar entre sí el mecanismo de cooperación, y las autoridades de control interesadas pueden prestarse asistencia mutua y realizar entre sí operaciones conjuntas, sobre una base bilateral o multilateral, sin tener que aplicarlo.

(139) A fin de fomentar la aplicación coherente del presente Reglamento, el Comité debe constituirse como organismo independiente de la Unión. Para cumplir sus objetivos, el Comité debe tener personalidad jurídica. Su presidente debe ostentar su representación. El Comité debe sustituir al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales creado por la Directiva 95/46/CE. Debe estar compuesto por el director de una autoridad de control de cada Estado miembro y el Supervisor Europeo de

Protección de Datos, o por sus respectivos representantes. La Comisión debe participar en las actividades del Comité sin derecho a voto y se deben reconocer derechos de voto específicos al Supervisor Europeo de Protección de Datos. El Comité debe contribuir a la aplicación coherente del presente Reglamento en toda la Unión, entre otras cosas asesorando a la Comisión, en particular sobre el nivel de protección en terceros países u organizaciones internacionales, y fomentando la cooperación de las autoridades de control en toda la Unión. El Comité debe actuar con independencia en el cumplimiento de sus funciones.

(140) El Comité debe contar con una secretaría, a cargo el Supervisor Europeo de Protección de Datos. El personal del Supervisor Europeo de Protección de Datos que participe en la realización de las funciones conferidas al Comité por el presente Reglamento debe desempeñar sus funciones siguiendo exclusivamente las instrucciones del presidente del Comité y responder ante él.

(141) Todo interesado debe tener derecho a presentar una reclamación ante una autoridad de control única, en particular en el Estado miembro de su residencia habitual, y derecho a la tutela judicial efectiva de conformidad con el artículo 47 de la Carta si considera que se vulneran sus derechos con arreglo al presente Reglamento o en caso de que la autoridad de control no responda a una reclamación, rechace o desestime total o parcialmente una reclamación o no actúe cuando sea necesario para proteger los derechos del interesado. La investigación a raíz de una reclamación debe llevarse a cabo, bajo control judicial, si procede en el caso concreto. La autoridad de control debe informar al interesado de la evolución y el resultado de la reclamación en un plazo razonable. Si el asunto requiere una mayor investigación o coordinación con otra autoridad de control, se debe facilitar información intermedia al interesado. Para facilitar la presentación de reclamaciones, cada autoridad de control debe adoptar medidas como el suministro de un formulario de reclamaciones, que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

(142) El interesado que considere vulnerados los derechos reconocidos por el presente Reglamento debe tener derecho a conferir mandato a una entidad, organización o asociación sin ánimo de lucro que esté constituida con arreglo al Derecho de un Estado miembro, tenga objetivos estatutarios que sean de interés público y actúe en el ámbito de la protección de los datos personales, para que presente en su nombre una reclamación ante la autoridad de control, ejerza el derecho a la tutela judicial en nombre de los interesados o, si así lo establece el Derecho del Estado miembro, ejerza el derecho a recibir una indemnización en nombre de estos. Un Estado miembro puede reconocer a tal entidad, organización o asociación el derecho a presentar en él una reclamación con independencia del mandato de un interesado y el derecho a la tutela judicial efectiva, cuando existan motivos para creer que se han vulnerado los derechos de un interesado como consecuencia de un tratamiento de datos personales que sea contrario al presente Reglamento. Esa entidad, organización o asociación no puede estar autorizada a reclamar una indemnización en nombre de un interesado al margen del mandato de este último.

(143) Toda persona física o jurídica tiene derecho a interponer ante el Tribunal de Justicia recurso de anulación de decisiones del Comité, en las condiciones establecidas en el artículo 263 del TFUE. Como destinatarias de dichas decisiones, las autoridades de control interesadas que quieran impugnarlas tienen que interponer recurso en el plazo de dos meses a partir del momento en que les fueron notificadas, de conformidad con el artículo 263 del TFUE. En caso de que las decisiones del Comité afecten directa e individualmente a un responsable, un encargado o al reclamante, estos pueden interponer recurso de anulación de dichas decisiones en el plazo de dos meses a partir de su publicación en el sitio web del Comité, de conformidad con el artículo 263 del TFUE. Sin perjuicio de lo dispuesto en el artículo 263 del TFUE, toda persona física o jurídica debe tener derecho a la tutela judicial efectiva ante el tribunal nacional competente contra las decisiones de una autoridad de control que produzcan efectos jurídicos que le afecten. Tales decisiones se refieren en particular al ejercicio de los poderes de investigación, corrección y autorización por parte de la autoridad de control o a la desestimación o rechazo de reclamaciones. No obstante, el derecho a la tutela judicial efectiva no incluye medidas adoptadas por las autoridades de control que no sean jurídicamente vinculantes, como los dictámenes publicados o el

asesoramiento facilitado por ellas. Las acciones contra una autoridad de control deben ejercitarse ante los tribunales del Estado miembro en el que esté establecida y tramitarse con arreglo al Derecho procesal de dicho Estado miembro. Dichos tribunales deben tener plena jurisdicción, incluida la competencia para examinar todos los elementos de hecho y de Derecho relativos a la causa de la que conozcan.

Si una autoridad de control rechaza o desestima una reclamación, el reclamante puede ejercitar una acción ante los tribunales del mismo Estado miembro. En el contexto de las acciones judiciales relacionadas con la aplicación del presente Reglamento, los tribunales nacionales que estimen necesaria una decisión al respecto para poder emitir su fallo pueden, o en el caso establecido en el artículo 267 del TFUE, deben solicitar al Tribunal de Justicia que se pronuncie con carácter prejudicial sobre la interpretación del Derecho de la Unión, incluido el presente Reglamento. Además, si una decisión de una autoridad de control por la que se ejecuta una decisión del Comité se impugna ante un tribunal nacional y se cuestiona la validez de la decisión del Comité, dicho tribunal nacional no es competente para declarar inválida la decisión del Comité, sino que, si la considera inválida, tiene que remitir la cuestión de la validez al Tribunal de Justicia de conformidad con el artículo 267 del TFUE, según la interpretación de este. No obstante, un tribunal nacional puede no remitir la cuestión de la validez de la decisión del Comité a instancia de una persona física o jurídica que, habiendo tenido la oportunidad de interponer recurso de anulación de dicha decisión, en particular si dicha decisión la afectaba directa e individualmente, no lo hizo en el plazo establecido en el artículo 263 del TFUE.

(144) Si un tribunal ante el cual se ejercitaron acciones contra una decisión de una autoridad de control tiene motivos para creer que se ejercitaron acciones ante un tribunal competente de otro Estado miembro relativas al mismo tratamiento, como tener el mismo asunto con respecto a un tratamiento por el mismo responsable o encargado, o la misma causa de la acción, debe ponerse en contacto con ese tribunal para confirmar la existencia de tales acciones conexas. Si dichas acciones conexas están pendientes ante un tribunal de otro Estado miembro, cualquier otro tribunal distinto de aquel ante el cual se ejercitó la acción en primer lugar puede suspender el procedimiento o, a instancia de una de las partes, inhibirse a favor del tribunal ante el cual se ejercitó la acción en primer lugar si este último es competente para su conocimiento y su acumulación es conforme a Derecho. Se consideran conexas las acciones vinculadas entre sí por una relación tan estrecha que procede tramitarlas y resolverlas conjuntamente a fin de evitar resoluciones que podrían ser incompatibles si se sustanciaran como causas separadas.

(145) Por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el interesado, a menos que el responsable sea una autoridad pública de un Estado miembro que actúe en el ejercicio de poderes públicos.

(146) El responsable o el encargado del tratamiento debe indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción del presente Reglamento. El responsable o el encargado deben quedar exentos de responsabilidad si se demuestra que en modo alguno son responsables de los daños y perjuicios. El concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia, de tal modo que se respeten plenamente los objetivos del presente Reglamento. Lo anterior se entiende sin perjuicio de cualquier reclamación por daños y perjuicios derivada de la vulneración de otras normas del Derecho de la Unión o de los Estados miembros. Un tratamiento en infracción del presente Reglamento también incluye aquel tratamiento que infringe actos delegados y de ejecución adoptados de conformidad con el presente Reglamento y el Derecho de los Estados miembros que especifique las normas del presente Reglamento. Los interesados deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos. Si los responsables o encargados participan en el mismo tratamiento, cada responsable o encargado debe ser considerado responsable de la totalidad de los daños y perjuicios. No obstante, si se acumulan en la misma causa de conformidad con el Derecho de los Estados miembros, la indemnización puede prorratearse en función de la responsabilidad de cada responsable o encargado por los daños y perjuicios causados por el tratamiento, siempre

que se garantice la indemnización total y efectiva del interesado que sufrió los daños y perjuicios. Todo responsable o encargado que haya abonado la totalidad de la indemnización puede interponer recurso posteriormente contra otros responsables o encargados que hayan participado en el mismo tratamiento.

(147) En los casos en que el presente Reglamento contiene normas específicas sobre competencia judicial, en particular por lo que respecta a las acciones que tratan de obtener satisfacción por la vía judicial, incluida la indemnización, contra un responsable o encargado del tratamiento, las normas generales de competencia judicial como las establecidas en el Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo [13] deben entenderse sin perjuicio de la aplicación de dichas normas específicas.

(148) A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

(149) Los Estados miembros deben tener la posibilidad de establecer normas en materia de sanciones penales por infracciones del presente Reglamento, incluidas las infracciones de normas nacionales adoptadas con arreglo a él y dentro de sus límites. Dichas sanciones penales pueden asimismo autorizar la privación de los beneficios obtenidos en infracción del presente Reglamento. No obstante, la imposición de sanciones penales por infracciones de dichas normas nacionales y de sanciones administrativas no debe entrañar la vulneración del principio ne bis in idem, según la interpretación del Tribunal de Justicia.

(150) A fin de reforzar y armonizar las sanciones administrativas por infracción del presente Reglamento, cada autoridad de control debe estar facultada para imponer multas administrativas. El presente Reglamento debe indicar las infracciones así como el límite máximo y los criterios para fijar las correspondientes multas administrativas, que la autoridad de control competente debe determinar en cada caso individual teniendo en cuenta todas las circunstancias concurrentes en él, atendiendo en particular a la naturaleza, gravedad y duración de la infracción y sus consecuencias y a las medidas tomadas para garantizar el cumplimiento de las obligaciones impuestas por el presente Reglamento e impedir o mitigar las consecuencias de la infracción. Si las multas administrativas se imponen a una empresa, por tal debe entenderse una empresa con arreglo a los artículos 101 y 102 del TFUE. Si las multas administrativas se imponen a personas que no son una empresa, la autoridad de control debe tener en cuenta al valorar la cuantía apropiada de la multa el nivel general de ingresos prevaleciente en el Estado miembro así como la situación económica de la persona. El mecanismo de coherencia también puede emplearse para fomentar una aplicación coherente de las multas administrativas. Debe corresponder a los Estados miembros determinar si y en qué medida se debe imponer multas administrativas a las autoridades públicas. La imposición de una multa administrativa o de una advertencia no afecta al ejercicio de otras competencias de las autoridades de control ni a la aplicación de otras sanciones al amparo del presente Reglamento.

(151) Los ordenamientos jurídicos de Dinamarca y Estonia no permiten las multas administrativas según lo dispuesto en el presente Reglamento. Las normas sobre multas administrativas pueden ser aplicadas en Dinamarca de tal manera que la multa sea impuesta por los tribunales nacionales competentes en cuanto sanción penal, y en Estonia de tal manera que la multa sea impuesta por la autoridad de control en el marco de un juicio de faltas, siempre que tal aplicación de las normas en dichos Estados miembros tenga un efecto

equivalente a las multas administrativas impuestas por las autoridades de control. Por lo tanto los tribunales nacionales competentes deben tener en cuenta la recomendación de la autoridad de control que incoe la multa. En todo caso, las multas impuestas deben ser efectivas, proporcionadas y disuasorias.

(152) En los casos en que el presente Reglamento no armoniza las sanciones administrativas, o en otros casos en que se requiera, por ejemplo en casos de infracciones graves del presente Reglamento, los Estados miembros deben aplicar un sistema que establezca sanciones efectivas, proporcionadas y disuasorias. La naturaleza de dichas sanciones, ya sea penal o administrativa, debe ser determinada por el Derecho de los Estados miembros.

(153) El Derecho de los Estados miembros debe conciliar las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria, con el derecho a la protección de los datos personales con arreglo al presente Reglamento. El tratamiento de datos personales con fines exclusivamente periodísticos o con fines de expresión académica, artística o literaria debe estar sujeto a excepciones o exenciones de determinadas disposiciones del presente Reglamento si así se requiere para conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información consagrado en el artículo 11 de la Carta. Esto debe aplicarse en particular al tratamiento de datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas. Por tanto, los Estados miembros deben adoptar medidas legislativas que establezcan las exenciones y excepciones necesarias para equilibrar estos derechos fundamentales. Los Estados miembros deben adoptar tales exenciones y excepciones con relación a los principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos. Si dichas exenciones o excepciones difieren de un Estado miembro a otro debe regir el Derecho del Estado miembro que sea aplicable al responsable del tratamiento. A fin de tener presente la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario que nociones relativas a dicha libertad, como el periodismo, se interpreten en sentido amplio.

(154) El presente Reglamento permite que, al aplicarlo, se tenga en cuenta el principio de acceso del público a los documentos oficiales. El acceso del público a documentos oficiales puede considerarse de interés público. Los datos personales de documentos que se encuentren en poder de una autoridad pública o un organismo público deben poder ser comunicados públicamente por dicha autoridad u organismo si así lo establece el Derecho de la Unión o los Estados miembros aplicable a dicha autoridad u organismo. Ambos Derechos deben conciliar el acceso del público a documentos oficiales y la reutilización de la información del sector público con el derecho a la protección de los datos personales y, por tanto, pueden establecer la necesaria conciliación con el derecho a la protección de los datos personales de conformidad con el presente Reglamento. La referencia a autoridades y organismos públicos debe incluir, en este contexto, a todas las autoridades u otros organismos a los que se aplica el Derecho de los Estados miembros sobre el acceso del público a documentos. La Directiva 2003/98/CE del Parlamento Europeo y del Consejo [(14)] no altera ni afecta en modo alguno al nivel de protección de las personas físicas con respecto al tratamiento de datos personales con arreglo a las disposiciones del Derecho de la Unión y los Estados miembros y, en particular, no altera las obligaciones ni los derechos establecidos en el presente Reglamento. En concreto, dicha Directiva no debe aplicarse a los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de datos personales, ni a partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización haya quedado establecida por ley como incompatible con el Derecho relativo a la protección de las personas físicas con respecto al tratamiento de los datos personales.

(155) El Derecho de los Estados miembros o los convenios colectivos, incluidos los «convenios de empresa», pueden establecer normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular en relación con las condiciones en las que los datos personales en el contexto laboral pueden ser objeto de tratamiento sobre la base del consentimiento del trabajador, los fines de la contratación, la

ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral.

(156) El tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos debe estar supeditado a unas garantías adecuadas para los derechos y libertades del interesado de conformidad con el presente Reglamento. Esas garantías deben asegurar que se aplican medidas técnicas y organizativas para que se observe, en particular, el principio de minimización de los datos. El tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas (como, por ejemplo, la seudonimización de datos). Los Estados miembros deben establecer garantías adecuadas para el tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Debe autorizarse que los Estados miembros establezcan, bajo condiciones específicas y a reserva de garantías adecuadas para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición, cuando se traten datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Las condiciones y garantías en cuestión pueden conllevar procedimientos específicos para que los interesados ejerzan dichos derechos si resulta adecuado a la luz de los fines perseguidos por el tratamiento específico, junto con las medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los principios de proporcionalidad y necesidad. El tratamiento de datos personales con fines científicos también debe observar otras normas pertinentes, como las relativas a los ensayos clínicos.

(157) Combinando información procedente de registros, los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión. Partiendo de registros, los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. Dentro de las ciencias sociales, la investigación basada en registros permite que los investigadores obtengan conocimientos esenciales acerca de la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales, como el desempleo y la educación. Los resultados de investigaciones obtenidos de registros proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basada en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la eficiencia de los servicios sociales. Para facilitar la investigación científica, los datos personales pueden tratarse con fines científicos, a reserva de condiciones y garantías adecuadas establecidas en el Derecho de la Unión o de los Estados miembros.

(158) El presente Reglamento también debe aplicarse al tratamiento de datos personales realizado con fines de archivo, teniendo presente que no debe se de aplicación a personas fallecidas. Las autoridades públicas o los organismos públicos o privados que llevan registros de interés público deben ser servicios que están obligados, con arreglo al Derecho de la Unión o de los Estados miembros, a adquirir, mantener, evaluar, organizar, describir, comunicar, promover y difundir registros de valor perdurable para el interés público general y facilitar acceso a ellos. Los Estados miembros también debe estar autorizados a establecer el tratamiento ulterior de datos personales con fines de archivo, por ejemplo a fin de ofrecer información específica relacionada con el comportamiento político bajo antiguos regímenes de Estados totalitarios, el genocidio, los crímenes contra la humanidad, en particular el Holocausto, o los crímenes de guerra.

(159) El presente Reglamento también debe aplicarse al tratamiento datos personales que se realice con fines de investigación científica. El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de

manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, debe tener en cuenta el objetivo de la Unión establecido en el artículo 179, apartado 1, del TFUE de realizar un espacio europeo de investigación. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública. Para cumplir las especificidades del tratamiento de datos personales con fines de investigación científica deben aplicarse condiciones específicas, en particular en lo que se refiere a la publicación o la comunicación de otro modo de datos personales en el contexto de fines de investigación científica. Si el resultado de la investigación científica, en particular en el ámbito de la salud, justifica otras medidas en beneficio del interesado, las normas generales del presente Reglamento deben aplicarse teniendo en cuenta tales medidas.

(160) El presente Reglamento debe aplicarse asimismo al tratamiento datos personales que se realiza con fines de investigación histórica. Esto incluye asimismo la investigación histórica y la investigación para fines genealógicos, teniendo en cuenta que el presente Reglamento no es de aplicación a personas fallecidas.

(161) Al objeto de otorgar el consentimiento para la participación en actividades de investigación científica en ensayos clínicos, deben aplicarse las disposiciones pertinentes del Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo [15].

(162) El presente Reglamento debe aplicarse al tratamiento de datos personales con fines estadísticos. El contenido estadístico, el control de accesos, las especificaciones para el tratamiento de datos personales con fines estadísticos y las medidas adecuadas para salvaguardar los derechos y las libertades de los interesados y garantizar la confidencialidad estadística deben ser establecidos, dentro de los límites del presente Reglamento, por el Derecho de la Unión o de los Estados miembros. Por fines estadísticos se entiende cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos. Estos resultados estadísticos pueden además utilizarse con diferentes fines, incluidos fines de investigación científica. El fin estadístico implica que el resultado del tratamiento con fines estadísticos no sean datos personales, sino datos agregados, y que este resultado o los datos personales no se utilicen para respaldar medidas o decisiones relativas a personas físicas concretas.

(163) Debe protegerse la información confidencial que las autoridades estadísticas de la Unión y nacionales recojan para la elaboración de las estadísticas oficiales europeas y nacionales. Las estadísticas europeas deben desarrollarse, elaborarse y difundirse con arreglo a los principios estadísticos fijados en el artículo 338, apartado 2, del TFUE, mientras que las estadísticas nacionales deben cumplir asimismo el Derecho de los Estados miembros. El Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo [16] facilita especificaciones adicionales sobre la confidencialidad estadística aplicada a las estadísticas europeas.

(164) Por lo que respecta a los poderes de las autoridades de control para obtener del responsable o del encargado del tratamiento acceso a los datos personales y a sus locales, los Estados miembros pueden adoptar por ley, dentro de los límites fijados por el presente Reglamento, normas específicas con vistas a salvaguardar el deber de secreto profesional u obligaciones equivalentes, en la medida necesaria para conciliar el derecho a la protección de los datos personales con el deber de secreto profesional. Lo anterior se entiende sin perjuicio de las obligaciones existentes para los Estados miembros de adoptar normas sobre el secreto profesional cuando así lo exija el Derecho de la Unión.

(165) El presente Reglamento respeta y no prejuzga el estatuto reconocido en los Estados miembros, en virtud del Derecho constitucional, a las iglesias y las asociaciones o comunidades religiosas, tal como se reconoce en el artículo 17 del TFUE.

(166) A fin de cumplir los objetivos del presente Reglamento, a saber, proteger los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, y garantizar la libre circulación de los datos personales en la Unión, debe delegarse en la Comisión el poder de adoptar actos de conformidad con el artículo 290 del TFUE. En particular, deben adoptarse actos delegados en relación con los criterios y requisitos para los mecanismos de certificación, la información que debe presentarse mediante iconos normalizados y los procedimientos para proporcionar

dichos iconos. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos. Al preparar y redactar los actos delegados, la Comisión debe garantizar la transmisión simultánea, oportuna y apropiada de los documentos pertinentes al Parlamento Europeo y al Consejo.

(167) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución cuando así lo establezca el presente Reglamento. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo. En este contexto, la Comisión debe considerar la adopción de medidas específicas para las microempresas y las pequeñas y medianas empresas.

(168) El procedimiento de examen debe seguirse para la adopción de actos de ejecución sobre cláusulas contractuales tipo entre responsables y encargados del tratamiento y entre responsables del tratamiento; códigos de conducta; normas técnicas y mecanismos de certificación; el nivel adecuado de protección ofrecido por un tercer país, un territorio o un sector específico en ese tercer país, o una organización internacional; cláusulas tipo de protección; formatos y procedimientos para el intercambio de información entre responsables, encargados y autoridades de control respecto de normas corporativas vinculantes; asistencia mutua; y modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre las autoridades de control y el Comité.

(169) La Comisión debe adoptar actos de ejecución inmediatamente aplicables cuando las pruebas disponibles muestren que un tercer país, un territorio o un sector específico en ese tercer país, o una organización internacional no garantizan un nivel de protección adecuado y así lo requieran razones imperiosas de urgencia.

(170) Dado que el objetivo del presente Reglamento, a saber, garantizar un nivel equivalente de protección de las personas físicas y la libre circulación de datos personales en la Unión Europea, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a las dimensiones o los efectos de la acción, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea (TUE). De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(171) La Directiva 95/46/CE debe ser derogada por el presente Reglamento. Todo tratamiento ya iniciado en la fecha de aplicación del presente Reglamento debe ajustarse al presente Reglamento en el plazo de dos años a partir de la fecha de su entrada en vigor. Cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del presente Reglamento, a fin de que el responsable pueda continuar dicho tratamiento tras la fecha de aplicación del presente Reglamento. Las decisiones de la Comisión y las autorizaciones de las autoridades de control basadas en la Directiva 95/46/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas.

(172) De conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.º 45/2001, se consultó al Supervisor Europeo de Protección de Datos, y éste emitió su dictamen el 7 de marzo de 2012 [17].

(173) El presente Reglamento debe aplicarse a todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales en relación con el tratamiento de datos personales que no están sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo [18], incluidas las obligaciones del responsable del tratamiento y los derechos de las personas físicas. Para aclarar la relación entre el presente Reglamento y la Directiva 2002/58/CE, esta última debe ser modificada en consecuencia. Una vez que se adopte el presente Reglamento, debe revisarse la Directiva 2002/58/CE, en particular con objeto de garantizar la coherencia con el presente Reglamento.

HAN ADOPTADO EL PRESENTE REGLAMENTO

(1) DO C 229 de 31.7.2012, p. 90.

(2) DO C 391 de 18.12.2012, p. 127.

(3) Posición del Parlamento Europeo de 12 de marzo de 2014 (pendiente de publicación en el Diario Oficial) y posición del Consejo en primera lectura de 8 de abril de 2016 (pendiente de publicación en el Diario Oficial). Posición del Parlamento Europeo de 14 de abril de 2016.

(4) Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

(5) Recomendación de la Comisión de 6 de mayo de 2003 sobre la definición de microempresas, pequeñas y medianas empresas [C(2003) 1422] (DO L 124 de 20.5.2003, p. 36).

(6) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

(7) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (véase la página 89 del presente Diario Oficial).

(8) Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO L 178 de 17.7.2000, p. 1).

(9) Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88 de 4.4.2011, p. 45).

(10) Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores (DO L 95 de 21.4.1993, p. 29).

(11) Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo (DO L 354 de 31.12.2008, p. 70).

(12) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

(13) Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (DO L 351 de 20.12.2012, p. 1).

(14) Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público (DO L 345 de 31.12.2003, p. 90).

(15) Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE (DO L 158 de 27.5.2014, p. 1).

(16) Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo, de 11 de marzo de 2009, relativo a la estadística europea y por el que se deroga el Reglamento (CE, Euratom) n.º 1101/2008 relativo a la transmisión a la Oficina Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico, el Reglamento (CE) n.º 322/97 del Consejo sobre la estadística comunitaria y la Decisión 89/382/CEE, Euratom del Consejo por la que se crea un Comité del programa estadístico de las Comunidades Europeas (DO L 87 de 31.3.2009, p. 164).

(17) DO C 192 de 30.6.2012, p. 7.

(18) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Artículo 2. *Ámbito de aplicación material.*

1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. El presente Reglamento no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;

b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;

c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

3. El Reglamento (CE) n.º 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98.

4. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15.

Artículo 3. *Ámbito territorial.*

1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que se encuentren en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.

Artículo 4. *Definiciones.*

A efectos del presente Reglamento se entenderá por:

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

3) «limitación del tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

6) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

9) «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

16) «establecimiento principal»:

a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;

b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;

17) «representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;

18) «empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;

19) «grupo empresarial»: grupo constituido por una empresa que ejerce el control y sus empresas controladas;

20) «normas corporativas vinculantes»: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

21) «autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;

22) «autoridad de control interesada»: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:

a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;

b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o

c) se ha presentado una reclamación ante esa autoridad de control;

23) «tratamiento transfronterizo»:

a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o

b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

24) «objeción pertinente y motivada»: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;

25) «servicio de la sociedad de la información»: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo [19];

26) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

---

[19] Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1).

CAPÍTULO II

Principios

Artículo 5. *Principios relativos al tratamiento.*

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Artículo 6. *Licitud del tratamiento.*

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa

requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

a) el Derecho de la Unión, o

b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Artículo 7. *Condiciones para el consentimiento.*

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Artículo 8. *Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.*

1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

Artículo 9. *Tratamiento de categorías especiales de datos personales.*

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Artículo 10. *Tratamiento de datos personales relativos a condenas e infracciones penales.*

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Artículo 11. *Tratamiento que no requiere identificación.*

1. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento.

2. Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

CAPÍTULO III

Derechos del interesado

Sección 1. Transparencia y modalidades

Artículo 12. *Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.*

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o

b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Sección 2. Información y acceso a los datos personales

Artículo 13. *Información que deberá facilitarse cuando los datos personales se obtengan del interesado.*

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.
4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 14. *Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.*

1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

d) las categorías de datos personales de que se trate;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;

b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;

c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;

e) el derecho a presentar una reclamación ante una autoridad de control;

f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:

a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;

b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o

c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;

b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable

adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;

c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

Artículo 15. *Derecho de acceso del interesado.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

Sección 3. Rectificación y supresión

Artículo 16. *Derecho de rectificación.*

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Artículo 17. *Derecho de supresión («el derecho al olvido»).*

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 18. *Derecho a la limitación del tratamiento.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Artículo 19. *Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento.*

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Artículo 20. *Derecho a la portabilidad de los datos.*

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Sección 4. Derecho de oposición y decisiones individuales automatizadas

Artículo 21. *Derecho de oposición.*

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Artículo 22. *Decisiones individuales automatizadas, incluida la elaboración de perfiles.*

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Sección 5. Limitaciones

Artículo 23. *Limitaciones.*

1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;

e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;

f) la protección de la independencia judicial y de los procedimientos judiciales;

g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);

i) la protección del interesado o de los derechos y libertades de otros;

j) la ejecución de demandas civiles.

2. En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:

a) la finalidad del tratamiento o de las categorías de tratamiento;

b) las categorías de datos personales de que se trate;

c) el alcance de las limitaciones establecidas;

d) las garantías para evitar accesos o transferencias ilícitos o abusivos;

e) la determinación del responsable o de categorías de responsables;

f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento;

g) los riesgos para los derechos y libertades de los interesados, y

h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.

CAPÍTULO IV

Responsable del tratamiento y encargado del tratamiento

Sección 1. Obligaciones generales

Artículo 24. *Responsabilidad del responsable del tratamiento.*

1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Artículo 25. *Protección de datos desde el diseño y por defecto.*

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Artículo 26. *Corresponsables del tratamiento.*

1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en

que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.

2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

Artículo 27. *Representantes de responsables o encargados del tratamiento no establecidos en la Unión.*

1. Cuando sea de aplicación el artículo 3, apartado 2, el responsable o el encargado del tratamiento designará por escrito un representante en la Unión.

2. La obligación establecida en el apartado 1 del presente artículo no será aplicable:

a) al tratamiento que sea ocasional, que no incluyan el manejo a gran escala de categorías especiales de datos indicadas en el artículo 9, apartado 1, o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o

b) a las autoridades u organismos públicos.

3. El representante estará establecido en uno de los Estados miembros en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado.

4. El responsable o el encargado del tratamiento encomendará al representante que atienda, junto al responsable o al encargado, o en su lugar, a las consultas, en particular, de las autoridades de control y de los interesados, sobre todos los asuntos relativos al tratamiento, a fin de garantizar el cumplimiento de lo dispuesto en el presente Reglamento.

5. La designación de un representante por el responsable o el encargado del tratamiento se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado.

Artículo 28. *Encargado del tratamiento.*

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.

7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.

9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Artículo 29. *Tratamiento bajo la autoridad del responsable o del encargado del tratamiento.*

El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 30. *Registro de las actividades de tratamiento.*

1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
b) los fines del tratamiento;
c) una descripción de las categorías de interesados y de las categorías de datos personales;
d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
b) las categorías de tratamientos efectuados por cuenta de cada responsable;
c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.
4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.
5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Artículo 31. *Cooperación con la autoridad de control.*

El responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones.

Sección 2. Seguridad de los datos personales

Artículo 32. *Seguridad del tratamiento.*

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.
4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 33. *Notificación de una violación de la seguridad de los datos personales a la autoridad de control.*

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.
2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 34. *Comunicación de una violación de la seguridad de los datos personales al interesado.*

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

Sección 3. Evaluación de impacto relativa a la protección de datos y consulta previa

Artículo 35. *Evaluación de impacto relativa a la protección de datos.*

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

Artículo 36. *Consulta previa.*

1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no

haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;

b) los fines y medios del tratamiento previsto;

c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;

d) en su caso, los datos de contacto del delegado de protección de datos;

e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y

f) cualquier otra información que solicite la autoridad de control.

4. Los Estados miembros garantizarán que se consulte a la autoridad de control durante la elaboración de toda propuesta de medida legislativa que haya de adoptar un Parlamento nacional, o de una medida reglamentaria basada en dicha medida legislativa, que se refiera al tratamiento.

5. No obstante lo dispuesto en el apartado 1, el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública.

Sección 4. Delegado de protección de datos

Artículo 37. *Designación del delegado de protección de datos.*

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos con arreglo al artículo 9 o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Artículo 38. *Posición del delegado de protección de datos.*

1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.

5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

Artículo 39. *Funciones del delegado de protección de datos.*

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Sección 5. Códigos de conducta y certificación

Artículo 40. *Códigos de conducta.*

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, como en lo que respecta a:

a) el tratamiento leal y transparente;

b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;

c) la recogida de datos personales;

d) la seudonimización de datos personales;

e) la información proporcionada al público y a los interesados;

f) el ejercicio de los derechos de los interesados;

g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;

h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;

i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;

j) la transferencia de datos personales a terceros países u organizaciones internacionales, o

k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79.

3. Además de la adhesión de los responsables o encargados del tratamiento a los que se aplica el presente Reglamento, los responsables o encargados a los que no se aplica el presente Reglamento en virtud del artículo 3 podrán adherirse también a códigos de conducta aprobados de conformidad con el apartado 5 del presente artículo y que tengan validez general en virtud del apartado 9 del presente artículo, a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra e). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

4. El código de conducta a que se refiere el apartado 2 del presente artículo contendrá mecanismos que permitan al organismo mencionado en el artículo 41, apartado 1, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes con arreglo al artículo 51 o 56.

5. Las asociaciones y otros organismos mencionados en el apartado 2 del presente artículo que proyecten elaborar un código de conducta o modificar o ampliar un código existente presentarán el proyecto de código o la modificación o ampliación a la autoridad de control que sea competente con arreglo al artículo 55. La autoridad de control dictaminará si el proyecto de código o la modificación o ampliación es conforme con el presente Reglamento y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.

6. Si el proyecto de código o la modificación o ampliación es aprobado de conformidad con el apartado 5 y el código de conducta de que se trate no se refiere a actividades de tratamiento en varios Estados miembros, la autoridad de control registrará y publicará el código.

7. Si un proyecto de código de conducta guarda relación con actividades de tratamiento en varios Estados miembros, la autoridad de control que sea competente en virtud del artículo 55 lo presentará por el procedimiento mencionado en el artículo 63, antes de su aprobación o de la modificación o ampliación, al Comité, el cual dictaminará si dicho proyecto, modificación o ampliación es conforme con el presente Reglamento o, en la situación indicada en el apartado 3 del presente artículo, ofrece garantías adecuadas.

8. Si el dictamen a que se refiere el apartado 7 confirma que el proyecto de código o la modificación o ampliación cumple lo dispuesto en el presente Reglamento o, en la situación indicada en el apartado 3, ofrece garantías adecuadas, el Comité presentará su dictamen a la Comisión.

9. La Comisión podrá, mediante actos de ejecución, decidir que el código de conducta o la modificación o ampliación aprobados y presentados con arreglo al apartado 8 del presente artículo tengan validez general dentro de la Unión. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

10. La Comisión dará publicidad adecuada a los códigos aprobados cuya validez general haya sido decidida de conformidad con el apartado 9.

11. El Comité archivará en un registro todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 41. *Supervisión de códigos de conducta aprobados.*

1. Sin perjuicio de las funciones y los poderes de la autoridad de control competente en virtud de los artículos 57 y 58, podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.

2. El organismo a que se refiere el apartado 1 podrá ser acreditado para supervisar el cumplimiento de un código de conducta si:

a) ha demostrado, a satisfacción de la autoridad de control competente, su independencia y pericia en relación con el objeto del código;

b) ha establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación;

c) ha establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y

d) ha demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

3. La autoridad de control competente someterá al Comité, con arreglo al mecanismo de coherencia a que se refiere el artículo 63, el proyecto que fije los requisitos de acreditación de un organismo a que se refiere el apartado 1 del presente artículo.

4. Sin perjuicio de las funciones y los poderes de la autoridad de control competente y de lo dispuesto en el capítulo VIII, un organismo a tenor del apartado 1 del presente artículo deberá, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y de las razones de las mismas a la autoridad de control competente.

5. La autoridad de control competente revocará la acreditación de un organismo a tenor del apartado 1 si los requisitos de acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe el presente Reglamento.

6. El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos.

Artículo 42. *Certificación.*

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

2. Además de la adhesión de los responsables o encargados del tratamiento sujetos al presente Reglamento, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el apartado 5, con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente Reglamento con arreglo al artículo 3 en el marco de transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra f). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

3. La certificación será voluntaria y estará disponible a través de un proceso transparente.

4. La certificación a que se refiere el presente artículo no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento y se entenderá sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes en virtud del artículo 55 o 56.

5. La certificación en virtud del presente artículo será expedida por los organismos de certificación a que se refiere el artículo 43 o por la autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad de conformidad con el artículo 58, apartado 3, o por el Comité de conformidad con el artículo 63. Cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos.

6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación dará al organismo de certificación mencionado en el artículo 43, o en su caso a la autoridad de control competente, toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación.

7. La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los criterios pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación a que se refiere el artículo 43, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los criterios para la certificación.

8. El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 43. *Organismo de certificación.*

1. Sin perjuicio de las funciones y poderes de la autoridad de control competente en virtud de los artículos 57 y 58, los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informada la autoridad de control, a fin de esta que pueda ejercer, si así se requiere, sus poderes en virtud del artículo 58, apartado 2, letra h). Los Estados miembros garantizarán que dichos organismos de certificación sean acreditados por la autoridad o el organismo indicado a continuación, o por ambos:

a) la autoridad de control que sea competente en virtud del artículo 55 o 56;

b) el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo [20] con arreglo a la norma EN ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la autoridad de control que sea competente en virtud del artículo 55 o 56.

2. Los organismos de certificación mencionados en el apartado 1 únicamente serán acreditados de conformidad con dicho apartado si:

a) han demostrado, a satisfacción de la autoridad de control competente, su independencia y su pericia en relación con el objeto de la certificación;

b) se han comprometido a respetar los criterios mencionados en el artículo 42, apartado 5, y aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56, o por el Comité de conformidad con el artículo 63;

c) han establecido procedimientos para la expedición, la revisión periódica y la retirada de certificaciones, sellos y marcas de protección de datos;

d) han establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación o a la manera en que la certificación haya sido o esté siendo aplicada por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y

e) han demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

3. La acreditación de los organismos de certificación a que se refieren los apartados 1 y 2 del presente artículo se realizará sobre la base de los requisitos aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56 o por el Comité en virtud del artículo 63. En caso de acreditación de conformidad con el apartado 1, letra b), del presente artículo, estos requisitos complementarán los contemplados en el Reglamento (CE) n.º 765/2008 y las normas técnicas que describen los métodos y procedimientos de los organismos de certificación.

4. Los organismos de certificación a que se refiere el apartado 1 serán responsable de la correcta evaluación a efectos de certificación o retirada de la certificación, sin perjuicio de la responsabilidad del responsable o del encargado del tratamiento en cuanto al cumplimiento del presente Reglamento. La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de certificación cumpla los requisitos establecidos en el presente artículo.

5. Los organismos de certificación a que se refiere el apartado 1 comunicarán a las autoridades de control competentes las razones de la expedición de la certificación solicitada o de su retirada.

6. La autoridad de control hará públicos los requisitos a que se refiere el apartado 3 del presente artículo y los criterios a que se refiere el artículo 42, apartado 5, en una forma fácilmente accesible. Las autoridades de control comunicarán también dichos requisitos y criterios al Comité.

7. No obstante lo dispuesto en el capítulo VIII, la autoridad de control competente o el organismo nacional de acreditación revocará la acreditación a un organismo de certificación a tenor del apartado 1 del presente artículo si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo de certificación infringe el presente Reglamento.

8. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 92, a fin de especificar las condiciones que deberán tenerse en cuenta para los mecanismos de certificación en materia de protección de datos a que se refiere el artículo 42, apartado 1.

9. La Comisión podrá adoptar actos de ejecución que establezcan normas técnicas para los mecanismos de certificación y los sellos y marcas de protección de datos, y mecanismos para promover y reconocer dichos mecanismos de certificación, sellos y marcas. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

---

[20] Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).

CAPÍTULO V

Transferencias de datos personales a terceros países u organizaciones internacionales

Artículo 44. *Principio general de las transferencias.*

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Artículo 45. *Transferencias basadas en una decisión de adecuación.*

1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y

c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que

se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE.

5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3.

6 La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5.

7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49.

8. La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo.

Artículo 46. *Transferencias mediante garantías adecuadas.*

1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:

a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

b) normas corporativas vinculantes de conformidad con el artículo 47;

c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;

d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;

e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o

f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o

b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo.

5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo.

Artículo 47. *Normas corporativas vinculantes.*

1. La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas:

a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y

c) cumplan los requisitos establecidos en el apartado 2.

2. Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos:

a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o

parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;

h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;

k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y

n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

3. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 48. *Transferencias o comunicaciones no autorizadas por el Derecho de la Unión.*

Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo.

Artículo 49. *Excepciones para situaciones específicas.*

1. En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;

c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;

d) la transferencia sea necesaria por razones importantes de interés público;

e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.

2. Una transferencia efectuada de conformidad con el apartado 1, párrafo primero, letra g), no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

3. En el apartado 1, el párrafo primero, letras a), b) y c), y el párrafo segundo no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

4. El interés público contemplado en el apartado 1, párrafo primero, letra d), será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

5. En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el Derecho de la Unión o de los Estados miembros podrá, por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional. Los Estados miembros notificarán a la Comisión dichas disposiciones.

6. El responsable o el encargado del tratamiento documentarán en los registros indicados en el artículo 30 la evaluación y las garantías apropiadas a que se refiere el apartado 1, párrafo segundo, del presente artículo.

Artículo 50. *Cooperación internacional en el ámbito de la protección de datos personales.*

En relación con los terceros países y las organizaciones internacionales, la Comisión y las autoridades de control tomarán medidas apropiadas para:

a) crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales;

b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales;

c) asociar a partes interesadas en la materia a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales;

d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

CAPÍTULO VI

Autoridades de control independientes

Sección 1. Independencia

Artículo 51. *Autoridad de control.*

1. Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.

2. Cada autoridad de control contribuirá a la aplicación coherente del presente Reglamento en toda la Unión. A tal fin, las autoridades de control cooperarán entre sí y con la Comisión con arreglo a lo dispuesto en el capítulo VII.

3. Cuando haya varias autoridades de control en un Estado miembro, este designará la autoridad de control que representará a dichas autoridades en el Comité, y establecerá el mecanismo que garantice el cumplimiento por las demás autoridades de las normas relativas al mecanismo de coherencia a que se refiere el artículo 63.

4. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el presente capítulo a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que afecte a dichas disposiciones.

Artículo 52. *Independencia.*

1. Cada autoridad de control actuará con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento.

2. El miembro o los miembros de cada autoridad de control serán ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento, a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción.

3. El miembro o los miembros de cada autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no.

4. Cada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité.

5. Cada Estado miembro garantizará que cada autoridad de control elija y disponga de su propio personal, que estará sujeto a la autoridad exclusiva del miembro o miembros de la autoridad de control interesada.

6. Cada Estado miembro garantizará que cada autoridad de control esté sujeta a un control financiero que no afecte a su independencia y que disponga de un presupuesto anual, público e independiente, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

Artículo 53. *Condiciones generales aplicables a los miembros de la autoridad de control.*

1. Los Estados miembros dispondrán que cada miembro de sus autoridades de control sea nombrado mediante un procedimiento transparente por:

— su Parlamento,
— su Gobierno,
— su Jefe de Estado, o
— un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros.

2. Cada miembro poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.

3. Los miembros darán por concluidas sus funciones en caso de terminación del mandato, dimisión o jubilación obligatoria, de conformidad con el Derecho del Estado miembro de que se trate.

4. Un miembro será destituido únicamente en caso de conducta irregular grave o si deja de cumplir las condiciones exigidas en el desempeño de sus funciones.

Artículo 54. *Normas relativas al establecimiento de la autoridad de control.*

1. Cada Estado miembro establecerá por ley todos los elementos indicados a continuación:

a) el establecimiento de cada autoridad de control;

b) las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de cada autoridad de control;

c) las normas y los procedimientos para el nombramiento del miembro o miembros de cada autoridad de control;

d) la duración del mandato del miembro o los miembros de cada autoridad de control, no inferior a cuatro años, salvo el primer nombramiento posterior al 24 de mayo de 2016, parte del cual podrá ser más breve cuando sea necesario para proteger la independencia de la autoridad de control por medio de un procedimiento de nombramiento escalonado;

e) el carácter renovable o no del mandato del miembro o los miembros de cada autoridad de control y, en su caso, el número de veces que podrá renovarse;

f) las condiciones por las que se rigen las obligaciones del miembro o los miembros y del personal de cada autoridad de control, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, y las normas que rigen el cese en el empleo.

2. El miembro o miembros y el personal de cada autoridad de control estarán sujetos, de conformidad con el Derecho de la Unión o de los Estados miembros, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus poderes. Durante su mandato, dicho deber de secreto profesional se aplicará en particular a la información recibida de personas físicas en relación con infracciones del presente Reglamento.

Sección 2. Competencia, funciones y poderes

Artículo 55. *Competencia.*

1. Cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro.

2. Cuando el tratamiento sea efectuado por autoridades públicas o por organismos privados que actúen con arreglo al artículo 6, apartado 1, letras c) o e), será competente la autoridad de control del Estado miembro de que se trate. No será aplicable en tales casos el artículo 56.

3. Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial.

Artículo 56. *Competencia de la autoridad de control principal.*

1. Sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60.

2. No obstante lo dispuesto en el apartado 1, cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro.

3. En los casos a que se refiere el apartado 2 del presente artículo, la autoridad de control informará sin dilación al respecto a la autoridad de control principal. En el plazo de tres semanas después de haber sido informada, la autoridad de control principal decidirá si tratará o no el caso de conformidad con el procedimiento establecido en el artículo 60, teniendo presente si existe un establecimiento del responsable o encargado del tratamiento en el Estado miembro de la autoridad de control que le haya informado.

4. En caso de que la autoridad de control principal decida tratar el caso, se aplicará el procedimiento establecido en el artículo 60. La autoridad de control que haya informado a la autoridad de control principal podrá presentarle un proyecto de decisión. La autoridad de control principal tendrá en cuenta en la mayor medida posible dicho proyecto al preparar el proyecto de decisión a que se refiere el artículo 60, apartado 3.

5. En caso de que la autoridad de control principal decida no tratar el caso, la autoridad de control que le haya informado lo tratará con arreglo a los artículos 61 y 62.

6. La autoridad de control principal será el único interlocutor del responsable o del encargado en relación con el tratamiento transfronterizo realizado por dicho responsable o encargado.

Artículo 57. *Funciones.*

1. Sin perjuicio de otras funciones en virtud del presente Reglamento, incumbirá a cada autoridad de control, en su territorio:

a) controlar la aplicación del presente Reglamento y hacerlo aplicar;

b) promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención;

c) asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento;

d) promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento;

e) previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros;

f) tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;

g) cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento;

h) llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública;

i) hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales;

j) adoptar las cláusulas contractuales tipo a que se refieren el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

k) elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos, en virtud del artículo 35, apartado 4;

l) ofrecer asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36, apartado 2;

m) alentar la elaboración de códigos de conducta con arreglo al artículo 40, apartado 1, y dictaminar y aprobar los códigos de conducta que den suficientes garantías con arreglo al artículo 40, apartado 5;

n) fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos con arreglo al artículo 42, apartado 1, y aprobar los criterios de certificación de conformidad con el artículo 42, apartado 5;

o) llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas en virtud del artículo 42, apartado 7;

p) elaborar y publicar los requisitos para la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

q) efectuar la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

r) autorizar las cláusulas contractuales y disposiciones a que se refiere el artículo 46, apartado 3;

s) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47;

t) contribuir a las actividades del Comité;

u) llevar registros internos de las infracciones del presente Reglamento y de las medidas adoptadas de conformidad con el artículo 58, apartado 2, y

v) desempeñar cualquier otra función relacionada con la protección de los datos personales.

2. Cada autoridad de control facilitará la presentación de las reclamaciones contempladas en el apartado 1, letra f), mediante medidas como un formulario de presentación de reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

3. El desempeño de las funciones de cada autoridad de control será gratuito para el interesado y, en su caso, para el delegado de protección de datos.

4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de control podrá establecer una tasa razonable basada en los costes administrativos o negarse a actuar respecto de la solicitud. La carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de control.

Artículo 58. *Poderes.*

1. Cada autoridad de control dispondrá de todos los poderes de investigación indicados a continuación:

a) ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones;

b) llevar a cabo investigaciones en forma de auditorías de protección de datos;

c) llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7;

d) notificar al responsable o al encargado del tratamiento las presuntas infracciones del presente Reglamento;

e) obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones;

f) obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros.

2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

a) sancionar a todo responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

c) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento;

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

e) ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;

f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;

g) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;

h) retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

3. Cada autoridad de control dispondrá de todos los poderes de autorización y consultivos indicados a continuación:

a) asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 36;

b) emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;

c) autorizar el tratamiento a que se refiere el artículo 36, apartado 5, si el Derecho del Estado miembro requiere tal autorización previa;

d) emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el artículo 40, apartado 5;

e) acreditar los organismos de certificación con arreglo al artículo 43;

f) expedir certificaciones y aprobar criterios de certificación con arreglo al artículo 42, apartado 5;

g) adoptar las cláusulas tipo de protección de datos contempladas en el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

h) autorizar las cláusulas contractuales indicadas en el artículo 46, apartado 3, letra a);

i) autorizar los acuerdos administrativos contemplados en el artículo 46, apartado 3, letra b);

j) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47.

4. El ejercicio de los poderes conferidos a la autoridad de control en virtud del presente artículo estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros de conformidad con la Carta.

5. Cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo.

6. Cada Estado miembro podrá establecer por ley que su autoridad de control tenga otros poderes además de los indicadas en los apartados 1, 2 y 3. El ejercicio de dichos poderes no será obstáculo a la aplicación efectiva del capítulo VII.

Artículo 59. *Informe de actividad.*

Cada autoridad de control elaborará un informe anual de sus actividades, que podrá incluir una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas de conformidad con el artículo 58, apartado 2. Los informes se transmitirán al Parlamento nacional, al Gobierno y a las demás autoridades designadas en virtud del Derecho de los Estados miembros. Se pondrán a disposición del público, de la Comisión y del Comité.

CAPÍTULO VII

Cooperación y coherencia

Sección 1. Cooperación y coherencia

Artículo 60. *Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas.*

1. La autoridad de control principal cooperará con las demás autoridades de control interesadas de acuerdo con el presente artículo, esforzándose por llegar a un consenso. La autoridad de control principal y las autoridades de control interesadas se intercambiarán toda información pertinente.

2. La autoridad de control principal podrá solicitar en cualquier momento a otras autoridades de control interesadas que presten asistencia mutua con arreglo al artículo 61, y podrá llevar a cabo operaciones conjuntas con arreglo al artículo 62, en particular para realizar investigaciones o supervisar la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro.

3. La autoridad de control principal comunicará sin dilación a las demás autoridades de control interesadas la información pertinente a este respecto. Transmitirá sin dilación un proyecto de decisión a las demás autoridades de control interesadas para obtener su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista.

4. En caso de que cualquiera de las autoridades de control interesadas formule una objeción pertinente y motivada acerca del proyecto de decisión en un plazo de cuatro semanas a partir de la consulta con arreglo al apartado 3 del presente artículo, la autoridad de control principal someterá el asunto, en caso de que no siga lo indicado en la objeción pertinente y motivada o estime que dicha objeción no es pertinente o no está motivada, al mecanismo de coherencia contemplado en el artículo 63.

5. En caso de que la autoridad de control principal prevea seguir lo indicado en la objeción pertinente y motivada recibida, presentará a dictamen de las demás autoridades de control interesadas un proyecto de decisión revisado. Dicho proyecto de decisión revisado se someterá al procedimiento indicado en el apartado 4 en un plazo de dos semanas.

6. En caso de que ninguna otra autoridad de control interesada haya presentado objeciones al proyecto de decisión transmitido por la autoridad de control principal en el

plazo indicado en los apartados 4 y 5, se considerará que la autoridad de control principal y las autoridades de control interesadas están de acuerdo con dicho proyecto de decisión y estarán vinculadas por este.

7. La autoridad de control principal adoptará y notificará la decisión al establecimiento principal o al establecimiento único del responsable o el encargado del tratamiento, según proceda, e informará de la decisión a las autoridades de control interesadas y al Comité, incluyendo un resumen de los hechos pertinentes y la motivación. La autoridad de control ante la que se haya presentado una reclamación informará de la decisión al reclamante.

8. No obstante lo dispuesto en el apartado 7, cuando se desestime o rechace una reclamación, la autoridad de control ante la que se haya presentado adoptará la decisión, la notificará al reclamante e informará de ello al responsable del tratamiento.

9. En caso de que la autoridad de control principal y las autoridades de control interesadas acuerden desestimar o rechazar determinadas partes de una reclamación y atender otras partes de ella, se adoptará una decisión separada para cada una de esas partes del asunto. La autoridad de control principal adoptará la decisión respecto de la parte referida a acciones en relación con el responsable del tratamiento, la notificará al establecimiento principal o al único establecimiento del responsable o del encargado en el territorio de su Estado miembro, e informará de ello al reclamante, mientras que la autoridad de control del reclamante adoptará la decisión respecto de la parte relativa a la desestimación o rechazo de dicha reclamación, la notificará a dicho reclamante e informará de ello al responsable o al encargado.

10. Tras recibir la notificación de la decisión de la autoridad de control principal con arreglo a los apartados 7 y 9, el responsable o el encargado del tratamiento adoptará las medidas necesarias para garantizar el cumplimiento de la decisión en lo tocante a las actividades de tratamiento en el contexto de todos sus establecimientos en la Unión. El responsable o el encargado notificarán las medidas adoptadas para dar cumplimiento a dicha decisión a la autoridad de control principal, que a su vez informará a las autoridades de control interesadas.

11. En circunstancias excepcionales, cuando una autoridad de control interesada tenga motivos para considerar que es urgente intervenir para proteger los intereses de los interesados, se aplicará el procedimiento de urgencia a que se refiere el artículo 66.

12. La autoridad de control principal y las demás autoridades de control interesadas se facilitarán recíprocamente la información requerida en el marco del presente artículo por medios electrónicos, utilizando un formulario normalizado.

Artículo 61. *Asistencia mutua.*

1. Las autoridades de control se facilitarán información útil y se prestarán asistencia mutua a fin de aplicar el presente Reglamento de manera coherente, y tomarán medidas para asegurar una efectiva cooperación entre ellas. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, como las solicitudes para llevar a cabo autorizaciones y consultas previas, inspecciones e investigaciones.

2. Cada autoridad de control adoptará todas las medidas oportunas requeridas para responder a una solicitud de otra autoridad de control sin dilación indebida y a más tardar en el plazo de un mes a partir de la solicitud. Dichas medidas podrán incluir, en particular, la transmisión de información pertinente sobre el desarrollo de una investigación.

3. Las solicitudes de asistencia deberán contener toda la información necesaria, entre otras cosas respecto de la finalidad y los motivos de la solicitud. La información que se intercambie se utilizará únicamente para el fin para el que haya sido solicitada.

4. La autoridad de control requerida no podrá negarse a responder a una solicitud, salvo si:

a) no es competente en relación con el objeto de la solicitud o con las medidas cuya ejecución se solicita, o

b) el hecho de responder a la solicitud infringiría el presente Reglamento o el Derecho de la Unión o de los Estados miembros que se aplique a la autoridad de control a la que se dirigió la solicitud.

5. La autoridad de control requerida informará a la autoridad de control requirente de los resultados obtenidos o, en su caso, de los progresos registrados o de las medidas adoptadas para responder a su solicitud. La autoridad de control requerida explicará los motivos de su negativa a responder a una solicitud al amparo del apartado 4.

6. Como norma general, las autoridades de control requeridas facilitarán la información solicitada por otras autoridades de control por medios electrónicos, utilizando un formato normalizado.

7. Las autoridades de control requeridas no cobrarán tasa alguna por las medidas adoptadas a raíz de una solicitud de asistencia mutua. Las autoridades de control podrán convenir normas de indemnización recíproca por gastos específicos derivados de la prestación de asistencia mutua en circunstancias excepcionales.

8. Cuando una autoridad de control no facilite la información mencionada en el apartado 5 del presente artículo en el plazo de un mes a partir de la recepción de la solicitud de otra autoridad de control, la autoridad de control requirente podrá adoptar una medida provisional en el territorio de su Estado miembro de conformidad con lo dispuesto en el artículo 55, apartado 1. En ese caso, se supondrá que existe la necesidad urgente contemplada en el artículo 66, apartado 1, que exige una decisión urgente y vinculante del Comité en virtud del artículo 66, apartado 2.

9. La Comisión podrá, mediante actos de ejecución, especificar el formato y los procedimientos de asistencia mutua contemplados en el presente artículo, así como las modalidades del intercambio de información por medios electrónicos entre las autoridades de control y entre las autoridades de control y el Comité, en especial el formato normalizado mencionado en el apartado 6 del presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 62. *Operaciones conjuntas de las autoridades de control.*

1. Las autoridades de control realizarán, en su caso, operaciones conjuntas, incluidas investigaciones conjuntas y medidas de ejecución conjuntas, en las que participen miembros o personal de las autoridades de control de otros Estados miembros.

2. Si el responsable o el encargado del tratamiento tiene establecimientos en varios Estados miembros o si es probable que un número significativo de interesados en más de un Estado miembro se vean sustancialmente afectados por las operaciones de tratamiento, una autoridad de control de cada uno de esos Estados miembros tendrá derecho a participar en operaciones conjuntas. La autoridad de control que sea competente en virtud del artículo 56, apartados 1 o 4, invitará a la autoridad de control de cada uno de dichos Estados miembros a participar en las operaciones conjuntas y responderá sin dilación a la solicitud de participación presentada por una autoridad de control.

3. Una autoridad de control podrá, con arreglo al Derecho de su Estado miembro y con la autorización de la autoridad de control de origen, conferir poderes, incluidos poderes de investigación, a los miembros o al personal de la autoridad de control de origen que participen en operaciones conjuntas, o aceptar, en la medida en que lo permita el Derecho del Estado miembro de la autoridad de control de acogida, que los miembros o el personal de la autoridad de control de origen ejerzan sus poderes de investigación de conformidad con el Derecho del Estado miembro de la autoridad de control de origen. Dichos poderes de investigación solo podrán ejercerse bajo la orientación y en presencia de miembros o personal de la autoridad de control de acogida. Los miembros o el personal de la autoridad de control de origen estarán sujetos al Derecho del Estado miembro de la autoridad de control de acogida.

4. Cuando participe, de conformidad con el apartado 1, personal de la autoridad de control de origen en operaciones en otro Estado miembro, el Estado miembro de la autoridad de control de acogida asumirá la responsabilidad de acuerdo con el Derecho del Estado miembro en cuyo territorio se desarrollen las operaciones, por los daños y perjuicios que haya causado dicho personal en el transcurso de las mismas.

5. El Estado miembro en cuyo territorio se causaron los daños y perjuicios asumirá su reparación en las condiciones aplicables a los daños y perjuicios causados por su propio personal. El Estado miembro de la autoridad de control de origen cuyo personal haya

causado daños y perjuicios a cualquier persona en el territorio de otro Estado miembro le restituirá íntegramente los importes que este último haya abonado a los derechohabientes.

6. Sin perjuicio del ejercicio de sus derechos frente a terceros y habida cuenta de la excepción establecida en el apartado 5, los Estados miembros renunciarán, en el caso contemplado en el apartado 1, a solicitar de otro Estado miembro el reembolso del importe de los daños y perjuicios mencionados en el apartado 4.

7. Cuando se prevea una operación conjunta y una autoridad de control no cumpla en el plazo de un mes con la obligación establecida en el apartado 2, segunda frase, del presente artículo, las demás autoridades de control podrán adoptar una medida provisional en el territorio de su Estado miembro de conformidad con el artículo 55. En ese caso, se presumirá la existencia de una necesidad urgente a tenor del artículo 66, apartado 1, y se requerirá dictamen o decisión vinculante urgente del Comité en virtud del artículo 66, apartado 2.

Sección 2. Coherencia

Artículo 63. *Mecanismo de coherencia.*

A fin de contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, en el marco del mecanismo de coherencia establecido en la presente sección.

Artículo 64. *Dictamen del Comité.*

1. El Comité emitirá un dictamen siempre que una autoridad de control competente proyecte adoptar alguna de las medidas enumeradas a continuación. A tal fin, la autoridad de control competente comunicará el proyecto de decisión al Comité, cuando la decisión:

a) tenga por objeto adoptar una lista de las operaciones de tratamiento supeditadas al requisito de la evaluación de impacto relativa a la protección de datos de conformidad con el artículo 35, apartado 4;

b) afecte a un asunto de conformidad con el artículo 40, apartado 7, cuyo objeto sea determinar si un proyecto de código de conducta o una modificación o ampliación de un código de conducta es conforme con el presente Reglamento;

c) tenga por objeto aprobar los requisitos para la acreditación de un organismo con arreglo al artículo 41, apartado 3, de un organismo de certificación conforme al artículo 43, apartado 3, o los criterios aplicables a la certificación a que se refiere el artículo 42, apartado 5;

d) tenga por objeto determinar las cláusulas tipo de protección de datos contempladas en el artículo 46, apartado 2, letra d), y el artículo 28, apartado 8;

e) tenga por objeto autorizar las cláusulas contractuales a que se refiere el artículo 46, apartado 3, letra a);

f) tenga por objeto la aprobación de normas corporativas vinculantes a tenor del artículo 47.

2. Cualquier autoridad de control, el presidente del Comité o la Comisión podrán solicitar que cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro sea examinado por el Comité a efectos de dictamen, en particular cuando una autoridad de control competente incumpla las obligaciones relativas a la asistencia mutua con arreglo al artículo 61 o las operaciones conjuntas con arreglo al artículo 62.

3. En los casos a que se refieren los apartados 1 y 2, el Comité emitirá dictamen sobre el asunto que le haya sido presentado siempre que no haya emitido ya un dictamen sobre el mismo asunto. Dicho dictamen se adoptará en el plazo de ocho semanas por mayoría simple de los miembros del Comité. Dicho plazo podrá prorrogarse seis semanas más, teniendo en cuenta la complejidad del asunto. Por lo que respecta al proyecto de decisión a que se refiere el apartado 1 y distribuido a los miembros del Comité con arreglo al apartado 5, todo miembro que no haya presentado objeciones dentro de un plazo razonable indicado por el presidente se considerará conforme con el proyecto de decisión.

4. Las autoridades de control y la Comisión comunicarán sin dilación por vía electrónica al Comité, utilizando un formato normalizado, toda información útil, en particular, cuando proceda, un resumen de los hechos, el proyecto de decisión, los motivos por los que es necesaria tal medida, y las opiniones de otras autoridades de control interesadas.

5. La Presidencia del Comité informará sin dilación indebida por medios electrónicos:

a) a los miembros del Comité y a la Comisión de cualquier información pertinente que le haya sido comunicada, utilizando un formato normalizado. La secretaría del Comité facilitará, de ser necesario, traducciones de la información que sea pertinente, y

b) a la autoridad de control contemplada, en su caso, en los apartados 1 y 2 y a la Comisión del dictamen, y lo publicará.

6. La autoridad de control competente a que se refiere el apartado 1 no adoptará su proyecto de decisión a tenor del apartado 1 en el plazo mencionado en el apartado 3.

7. La autoridad de control competente a que se refiere el apartado 1 tendrá en cuenta en la mayor medida posible el dictamen del Comité y, en el plazo de dos semanas desde la recepción del dictamen, comunicará por medios electrónicos al presidente del Comité si va a mantener o modificar su proyecto de decisión y, si lo hubiera, el proyecto de decisión modificado, utilizando un formato normalizado.

8. Cuando la autoridad de control competente a que se refiere el apartado 1 informe al presidente del Comité, en el plazo mencionado en el apartado 7 del presente artículo, de que no prevé seguir el dictamen del Comité, en todo o en parte, alegando los motivos correspondientes, se aplicará el artículo 65, apartado 1.

Artículo 65. *Resolución de conflictos por el Comité.*

1. Con el fin de garantizar una aplicación correcta y coherente del presente Reglamento en casos concretos, el Comité adoptará una decisión vinculante en los siguientes casos:

a) cuando, en un caso mencionado en el artículo 60, apartado 4, una autoridad de control interesada haya manifestado una objeción pertinente y motivada a un proyecto de decisión de la autoridad de control principal y esta no haya seguido la objeción o haya rechazado dicha objeción por no ser pertinente o no estar motivada. La decisión vinculante afectará a todos los asuntos a que se refiera la objeción pertinente y motivada, en particular si hay infracción del presente Reglamento;

b) cuando haya puntos de vista enfrentados sobre cuál de las autoridades de control interesadas es competente para el establecimiento principal;

c) cuando una autoridad de control competente no solicite dictamen al Comité en los casos contemplados en el artículo 64, apartado 1, o no siga el dictamen del Comité emitido en virtud del artículo 64. En tal caso, cualquier autoridad de control interesada, o la Comisión, lo pondrá en conocimiento del Comité.

2. La decisión a que se refiere el apartado 1 se adoptará en el plazo de un mes a partir de la remisión del asunto, por mayoría de dos tercios de los miembros del Comité. Este plazo podrá prorrogarse un mes más, habida cuenta de la complejidad del asunto. La decisión que menciona el apartado 1 estará motivada y será dirigida a la autoridad de control principal y a todas las autoridades de control interesadas, y será vinculante para ellas.

3. Cuando el Comité no haya podido adoptar una decisión en los plazos mencionados en el apartado 2, adoptará su decisión en un plazo de dos semanas tras la expiración del segundo mes a que se refiere el apartado 2, por mayoría simple de sus miembros. En caso de empate, decidirá el voto del presidente.

4. Las autoridades de control interesadas no adoptarán decisión alguna sobre el asunto presentado al Comité en virtud del apartado 1 durante los plazos de tiempo a que se refieren los apartados 2 y 3.

5. El presidente del Comité notificará sin dilación indebida la decisión contemplada en el apartado 1 a las autoridades de control interesadas. También informará de ello a la Comisión. La decisión se publicará en el sitio web del Comité sin demora, una vez que la autoridad de control haya notificado la decisión definitiva a que se refiere el apartado 6.

6. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación adoptará su decisión definitiva sobre la base de la decisión

contemplada en el apartado 1 del presente artículo, sin dilación indebida y a más tardar un mes tras la notificación de la decisión del Comité. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación informará al Comité de la fecha de notificación de su decisión definitiva al responsable o al encargado del tratamiento y al interesado, respectivamente. La decisión definitiva de las autoridades de control interesadas será adoptada en los términos establecidos en el artículo 60, apartados 7, 8 y 9. La decisión definitiva hará referencia a la decisión contemplada en el apartado 1 del presente artículo y especificará que esta última decisión se publicará en el sitio web del Comité con arreglo al apartado 5 del presente artículo. La decisión definitiva llevará adjunta la decisión contemplada en el apartado 1 del presente artículo.

Artículo 66. *Procedimiento de urgencia.*

1. En circunstancias excepcionales, cuando una autoridad de control interesada considere que es urgente intervenir para proteger los derechos y las libertades de interesados, podrá, como excepción al mecanismo de coherencia contemplado en los artículos 63, 64 y 65, o al procedimiento mencionado en el artículo 60, adoptar inmediatamente medidas provisionales destinadas a producir efectos jurídicos en su propio territorio, con un periodo de validez determinado que no podrá ser superior a tres meses. La autoridad de control comunicará sin dilación dichas medidas, junto con los motivos de su adopción, a las demás autoridades de control interesadas, al Comité y a la Comisión.

2. Cuando una autoridad de control haya adoptado una medida de conformidad con el apartado 1, y considere que deben adoptarse urgentemente medidas definitivas, podrá solicitar con carácter urgente un dictamen o una decisión vinculante urgente del Comité, motivando dicha solicitud de dictamen o decisión.

3. Cualquier autoridad de control podrá solicitar, motivando su solicitud, y, en particular, la urgencia de la intervención, un dictamen urgente o una decisión vinculante urgente, según el caso, del Comité, cuando una autoridad de control competente no haya tomado una medida apropiada en una situación en la que sea urgente intervenir a fin de proteger los derechos y las libertades de los interesados.

4. No obstante lo dispuesto en el artículo 64, apartado 3, y en el artículo 65, apartado 2, los dictámenes urgentes o decisiones vinculantes urgentes contemplados en los apartados 2 y 3 del presente artículo se adoptarán en el plazo de dos semanas por mayoría simple de los miembros del Comité.

Artículo 67. *Intercambio de información.*

La Comisión podrá adoptar actos de ejecución de ámbito general para especificar las modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre dichas autoridades y el Comité, en especial el formato normalizado contemplado en el artículo 64.

Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Sección 3. Comité europeo de protección de datos

Artículo 68. *Comité Europeo de Protección de Datos.*

1. Se crea el Comité Europeo de Protección de Datos («Comité»), como organismo de la Unión, que gozará de personalidad jurídica.

2. El Comité estará representado por su presidente.

3. El Comité estará compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos o sus representantes respectivos.

4. Cuando en un Estado miembro estén encargados de controlar la aplicación de las disposiciones del presente Reglamento varias autoridades de control, se nombrará a un representante común de conformidad con el Derecho de ese Estado miembro.

5. La Comisión tendrá derecho a participar en las actividades y reuniones del Comité, sin derecho a voto. La Comisión designará un representante. El presidente del Comité comunicará a la Comisión las actividades del Comité.

6. En los casos a que se refiere el artículo 65, el Supervisor Europeo de Protección de Datos sólo tendrá derecho a voto en las decisiones relativas a los principios y normas aplicables a las instituciones, órganos y organismos de la Unión que correspondan en cuanto al fondo a las contempladas en el presente Reglamento.

Artículo 69. *Independencia.*

1. El Comité actuará con total independencia en el desempeño de sus funciones o el ejercicio de sus competencias con arreglo a los artículos 70 y 71.

2. Sin perjuicio de las solicitudes de la Comisión contempladas en el artículo 70, apartados 1 y 2, el Comité no solicitará ni admitirá instrucciones de nadie en el desempeño de sus funciones o el ejercicio de sus competencias.

Artículo 70. *Funciones del Comité.*

1. El Comité garantizará la aplicación coherente del presente Reglamento. A tal efecto, el Comité, a iniciativa propia o, en su caso, a instancia de la Comisión, en particular:

a) supervisará y garantizará la correcta aplicación del presente Reglamento en los casos contemplados en los artículos 64 y 65, sin perjuicio de las funciones de las autoridades de control nacionales;

b) asesorará a la Comisión sobre toda cuestión relativa a la protección de datos personales en la Unión, en particular sobre cualquier propuesta de modificación del presente Reglamento;

c) asesorará a la Comisión sobre el formato y los procedimientos para intercambiar información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes;

d) emitirá directrices, recomendaciones y buenas prácticas relativas a los procedimientos para la supresión de vínculos, copias o réplicas de los datos personales procedentes de servicios de comunicación a disposición pública a que se refiere el artículo 17, apartado 2;

e) examinará, a iniciativa propia, a instancia de uno de sus miembros o de la Comisión, cualquier cuestión relativa a la aplicación del presente Reglamento, y emitirá directrices, recomendaciones y buenas prácticas a fin de promover la aplicación coherente del presente Reglamento;

f) emitirá directrices, recomendaciones y buenas prácticas de conformidad con la letra e) del presente apartado a fin de especificar más los criterios y requisitos de las decisiones basadas en perfiles en virtud del artículo 22, apartado 2;

g) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de constatar las violaciones de la seguridad de los datos y determinar la dilación indebida a tenor del artículo 33, apartados 1 y 2, y con respecto a las circunstancias particulares en las que el responsable o el encargado del tratamiento debe notificar la violación de la seguridad de los datos personales;

h) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado con respecto a las circunstancias en las que sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas a tenor del artículo 34, apartado 1;

i) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado con el fin de especificar en mayor medida los criterios y requisitos para las transferencias de datos personales basadas en normas corporativas vinculantes a las que se hayan adherido los responsables del tratamiento y en normas corporativas vinculantes a las que se hayan adherido los encargados del tratamiento y en requisitos adicionales necesarios para garantizar la protección de los datos personales de los interesados a que se refiere el artículo 47;

j) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de especificar en mayor medida los criterios y requisitos de las transferencias de datos personales sobre la base del artículo 49, apartado 1;

k) formulará directrices para las autoridades de control, relativas a la aplicación de las medidas a que se refiere el artículo 58, apartados 1, 2 y 3, y la fijación de multas administrativas de conformidad con el artículo 83;

l) examinará la aplicación práctica de las directrices, recomendaciones y buenas prácticas;

m) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de establecer procedimientos comunes de información procedente de personas físicas sobre infracciones del presente Reglamento en virtud del artículo 54, apartado 2;

n) alentará la elaboración de códigos de conducta y el establecimiento de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos de conformidad con los artículos 40 y 42;

o) aprobará los criterios de certificación en virtud del artículo 42, apartado 5, y llevará un registro público de los mecanismos de certificación y sellos y marcas de protección de datos en virtud del artículo 42, apartado 8, y de los responsables o los encargados del tratamiento certificados establecidos en terceros países en virtud del artículo 42, apartado 7;

p) aprobará los requisitos contemplados en el artículo 43, apartado 3, con miras a la acreditación de los organismos de certificación a los que se refiere el artículo 43;

q) facilitará a la Comisión un dictamen sobre los requisitos de certificación contemplados en el artículo 43, apartado 8;

r) facilitará a la Comisión un dictamen sobre los iconos a que se refiere el artículo 12, apartado 7;

s) facilitará a la Comisión un dictamen para evaluar la adecuación del nivel de protección en un tercer país u organización internacional, en particular para evaluar si un tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o una organización internacional, ya no garantizan un nivel de protección adecuado. A tal fin, la Comisión facilitará al Comité toda la documentación necesaria, incluida la correspondencia con el gobierno del tercer país, que se refiera a dicho tercer país, territorio o específico o a dicha organización internacional;

t) emitirá dictámenes sobre los proyectos de decisión de las autoridades de control en virtud del mecanismo de coherencia mencionado en el artículo 64, apartado 1, sobre los asuntos presentados en virtud del artículo 64, apartado 2, y sobre las decisiones vinculantes en virtud del artículo 65, incluidos los casos mencionados en el artículo 66;

u) promoverá la cooperación y los intercambios bilaterales y multilaterales efectivos de información y de buenas prácticas entre las autoridades de control;

v) promoverá programas de formación comunes y facilitará intercambios de personal entre las autoridades de control y, cuando proceda, con las autoridades de control de terceros países o con organizaciones internacionales;

w) promoverá el intercambio de conocimientos y documentación sobre legislación y prácticas en materia de protección de datos con las autoridades de control encargadas de la protección de datos a escala mundial;

x) emitirá dictámenes sobre los códigos de conducta elaborados a escala de la Unión de conformidad con el artículo 40, apartado 9, y

y) llevará un registro electrónico, de acceso público, de las decisiones adoptadas por las autoridades de control y los tribunales sobre los asuntos tratados en el marco del mecanismo de coherencia.

2. Cuando la Comisión solicite asesoramiento del Comité podrá señalar un plazo teniendo en cuenta la urgencia del asunto.

3. El Comité transmitirá sus dictámenes, directrices, recomendaciones y buenas prácticas a la Comisión y al Comité contemplado en el artículo 93, y los hará públicos.

4. Cuando proceda, el Comité consultará a las partes interesadas y les dará la oportunidad de presentar sus comentarios en un plazo razonable. Sin perjuicio de lo dispuesto en el artículo 76, el Comité publicará los resultados del procedimiento de consulta.

Artículo 71. *Informes.*

1. El Comité elaborará un informe anual en materia de protección de las personas físicas en lo que respecta al tratamiento en la Unión y, si procede, en terceros países y organizaciones internacionales. El informe se hará público y se transmitirá al Parlamento Europeo, al Consejo y a la Comisión.

2. El informe anual incluirá un examen de la aplicación práctica de las directrices, recomendaciones y buenas prácticas indicadas en el artículo 70, apartado 1, letra l), así como de las decisiones vinculantes indicadas en el artículo 65.

Artículo 72. *Procedimiento.*

1. El Comité tomará sus decisiones por mayoría simple de sus miembros, salvo que el presente Reglamento disponga otra cosa.

2. El Comité adoptará su reglamento interno por mayoría de dos tercios de sus miembros y organizará sus disposiciones de funcionamiento.

Artículo 73. *Presidencia.*

1. El Comité elegirá por mayoría simple de entre sus miembros un presidente y dos vicepresidentes.

2. El mandato del presidente y de los vicepresidentes será de cinco años de duración y podrá renovarse una vez.

Artículo 74. *Funciones del presidente.*

1. El presidente desempeñará las siguientes funciones:

a) convocar las reuniones del Comité y preparar su orden del día;

b) notificar las decisiones adoptadas por el Comité con arreglo al artículo 65 a la autoridad de control principal y a las autoridades de control interesadas;

c) garantizar el ejercicio puntual de las funciones del Comité, en particular en relación con el mecanismo de coherencia a que se refiere el artículo 63.

2. El Comité determinará la distribución de funciones entre el presidente y los vicepresidentes en su reglamento interno.

Artículo 75. *Secretaría.*

1. El Comité contará con una secretaría, de la que se hará cargo el Supervisor Europeo de Protección de Datos.

2. La secretaría ejercerá sus funciones siguiendo exclusivamente las instrucciones del presidente del Comité.

3. El personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento dependerá de un superior jerárquico distinto del personal que desempeñe las funciones conferidas al Supervisor Europeo de Protección de Datos.

4. El Comité, en consulta con el Supervisor Europeo de Protección de Datos, elaborará y publicará, si procede, un memorando de entendimiento para la puesta en práctica del presente artículo, que determinará los términos de su cooperación y que será aplicable al personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento.

5. La secretaría prestará apoyo analítico, administrativo y logístico al Comité.

6. La secretaría será responsable, en particular, de:

a) los asuntos corrientes del Comité;

b) la comunicación entre los miembros del Comité, su presidente y la Comisión;

c) la comunicación con otras instituciones y con el público;

d) la utilización de medios electrónicos para la comunicación interna y externa;

e) la traducción de la información pertinente;

f) la preparación y el seguimiento de las reuniones del Comité;

g) la preparación, redacción y publicación de dictámenes, decisiones relativas a solución de diferencias entre autoridades de control y otros textos adoptados por el Comité.

Artículo 76. *Confidencialidad.*

1. Los debates del Comité serán confidenciales cuando el mismo lo considere necesario, tal como establezca su reglamento interno.

2. El acceso a los documentos presentados a los miembros del Comité, los expertos y los representantes de terceras partes se regirá por el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo [21].

[21] Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

CAPÍTULO VIII

Recursos, responsabilidad y sanciones

Artículo 77. *Derecho a presentar una reclamación ante una autoridad de control.*

1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el presente Reglamento.

2. La autoridad de control ante la que se haya presentado la reclamación informará al reclamante sobre el curso y el resultado de la reclamación, inclusive sobre la posibilidad de acceder a la tutela judicial en virtud del artículo 78.

Artículo 78. *Derecho a la tutela judicial efectiva contra una autoridad de control.*

1. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna.

2. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, todo interesado tendrá derecho a la tutela judicial efectiva en caso de que la autoridad de control que sea competente en virtud de los artículos 55 y 56 no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación presentada en virtud del artículo 77.

3. Las acciones contra una autoridad de control deberán ejercitarse ante los tribunales del Estado miembro en que esté establecida la autoridad de control.

4. Cuando se ejerciten acciones contra una decisión de una autoridad de control que haya sido precedida de un dictamen o una decisión del Comité en el marco del mecanismo de coherencia, la autoridad de control remitirá al tribunal dicho dictamen o decisión.

Artículo 79. *Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento.*

1. Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del artículo 77, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales.

2. Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el

responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

Artículo 80. *Representación de los interesados.*

1. El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro.

2. Cualquier Estado miembro podrán disponer que cualquier entidad, organización o asociación mencionada en el apartado 1 del presente artículo tenga, con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control que sea competente en virtud del artículo 77 y a ejercer los derechos contemplados en los artículos 78 y 79, si considera que los derechos del interesado con arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento.

Artículo 81. *Suspensión de los procedimientos.*

1. Cuando un tribunal competente de un Estado miembro tenga información de la pendencia ante un tribunal de otro Estado miembro de un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado, se pondrá en contacto con dicho tribunal de otro Estado miembro para confirmar la existencia de dicho procedimiento.

2. Cuando un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado esté pendiente ante un tribunal de otro Estado miembro, cualquier tribunal competente distinto de aquel ante el que se ejercitó la acción en primer lugar podrá suspender su procedimiento.

3. Cuando dicho procedimiento esté pendiente en primera instancia, cualquier tribunal distinto de aquel ante el que se ejercitó la acción en primer lugar podrá también, a instancia de una de las partes, inhibirse en caso de que el primer tribunal sea competente para su conocimiento y su acumulación sea conforme a Derecho.

Artículo 82. *Derecho a indemnización y responsabilidad.*

1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.

3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.

4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.

5. Cuando, de conformidad con el apartado 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o

encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el apartado 2.

6. Las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2.

Artículo 83. *Condiciones generales para la imposición de multas administrativas.*

1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4.

5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

6. El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

8. El ejercicio por una autoridad de control de sus poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

9. Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. Los Estados miembros de que se trate notificarán a la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable.

Artículo 84. *Sanciones.*

1. Los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias.

2. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que les sea aplicable.

CAPÍTULO IX

Disposiciones relativas a situaciones específicas de tratamiento

Artículo 85. *Tratamiento y libertad de expresión y de información.*

1. Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.

2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o

excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.

3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas.

Artículo 86. *Tratamiento y acceso del público a documentos oficiales.*

Los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento.

Artículo 87. *Tratamiento del número nacional de identificación.*

Los Estados miembros podrán determinar adicionalmente las condiciones específicas para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general. En ese caso, el número nacional de identificación o cualquier otro medio de identificación de carácter general se utilizará únicamente con las garantías adecuadas para los derechos y las libertades del interesado con arreglo al presente Reglamento.

Artículo 88. *Tratamiento en el ámbito laboral.*

1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

3. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Artículo 89. *Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.*

1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

2. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos 15, 16, 18 y 21, sujetas a las condiciones y garantías indicadas en el apartado 1 del presente artículo, siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.

3. Cuando se traten datos personales con fines de archivo en interés público, el Derecho de le Unión o de los Estados miembros podrá prever excepciones a los derechos contemplados en los artículos 15, 16, 18, 19, 20 y 21, sujetas a las condiciones y garantías citadas en el apartado 1 del presente artículo, siempre que esos derechos puedan imposibilitar u obstaculizar gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.

4. En caso de que el tratamiento a que hacen referencia los apartados 2 y 3 sirva también al mismo tiempo a otro fin, las excepciones solo serán aplicables al tratamiento para los fines mencionados en dichos apartados.

Artículo 90. *Obligaciones de secreto.*

1. Los Estados miembros podrán adoptar normas específicas para fijar los poderes de las autoridades de control establecidos en el artículo 58, apartado 1, letras e) y f), en relación con los responsables o encargados sujetos, con arreglo al Derecho de la Unión o de los Estados miembros o a las normas establecidas por los organismos nacionales competentes, a una obligación de secreto profesional o a otras obligaciones de secreto equivalentes, cuando sea necesario y proporcionado para conciliar el derecho a la protección de los datos personales con la obligación de secreto. Esas normas solo se aplicarán a los datos personales que el responsable o el encargado del tratamiento hayan recibido como resultado o con ocasión de una actividad cubierta por la citada obligación de secreto.

2. Cada Estado miembro notificará a la Comisión las normas adoptadas de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Artículo 91. *Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas.*

1. Cuando en un Estado miembro iglesias, asociaciones o comunidades religiosas apliquen, en el momento de la entrada en vigor del presente Reglamento, un conjunto de normas relativas a la protección de las personas físicas en lo que respecta al tratamiento, tales normas podrán seguir aplicándose, siempre que sean conformes con el presente Reglamento.

2. Las iglesias y las asociaciones religiosas que apliquen normas generales de conformidad con el apartado 1 del presente artículo estarán sujetas al control de una autoridad de control independiente, que podrá ser específica, siempre que cumpla las condiciones establecidas en el capítulo VI del presente Reglamento.

CAPÍTULO X

Actos delegados y actos de ejecución

Artículo 92. *Ejercicio de la delegación.*

1. Los poderes para adoptar actos delegados otorgados a la Comisión estarán sujetos a las condiciones establecidas en el presente artículo.

2. La delegación de poderes indicada en el artículo 12, apartado 8, y en el artículo 43, apartado 8, se otorgarán a la Comisión por tiempo indefinido a partir del 24 de mayo de 2016.

3. La delegación de poderes mencionada en el artículo 12, apartado 8, y el artículo 43, apartado 8, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto al día siguiente de su publicación en el Diario

Oficial de la Unión Europea o en una fecha posterior indicada en la misma. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

5. Los actos delegados adoptados en virtud del artículo 12, apartado 8, y el artículo 43, apartado 8, entrarán en vigor únicamente si, en un plazo de tres meses desde su notificación al Parlamento Europeo y al Consejo, ni el Parlamento Europeo ni el Consejo formulan objeciones o si, antes del vencimiento de dicho plazo, tanto el uno como el otro informan a la Comisión de que no las formularán. El plazo se ampliará en tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 93. *Procedimiento de comité.*

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. Cuando se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

3. Cuando se haga referencia al presente apartado, se aplicará el artículo 8 del Reglamento (UE) n.º 182/2011, en relación con su artículo 5.

CAPÍTULO XI

Disposiciones finales

Artículo 94. *Derogación de la Directiva 95/46/CE.*

1. Queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018.

2. Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Comité Europeo de Protección de Datos establecido por el presente Reglamento.

Artículo 95. *Relación con la Directiva 2002/58/CE.*

El presente Reglamento no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE.

Artículo 96. *Relación con acuerdos celebrados anteriormente.*

Los acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales que hubieren sido celebrados por los Estados miembros antes del 24 de mayo de 2016 y que cumplan lo dispuesto en el Derecho de la Unión aplicable antes de dicha fecha, seguirán en vigor hasta que sean modificados, sustituidos o revocados.

Artículo 97. *Informes de la Comisión.*

1. A más tardar el 25 de mayo de 2020 y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. Los informes se harán públicos.

2. En el marco de las evaluaciones y revisiones a que se refiere el apartado 1, la Comisión examinará en particular la aplicación y el funcionamiento de:

a) el capítulo V sobre la transferencia de datos personales a países terceros u organizaciones internacionales, particularmente respecto de las decisiones adoptadas en virtud del artículo 45, apartado 3, del presente Reglamento, y de las adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE;

b) el capítulo VII sobre cooperación y coherencia.

3. A los efectos del apartado 1, la Comisión podrá solicitar información a los Estados miembros y a las autoridades de control.

4. Al llevar a cabo las evaluaciones y revisiones indicadas en los apartados 1 y 2, la Comisión tendrá en cuenta las posiciones y conclusiones del Parlamento Europeo, el Consejo y los demás órganos o fuentes pertinentes.

5. La Comisión presentará, en caso necesario, las propuestas oportunas para modificar el presente Reglamento, en particular teniendo en cuenta la evolución de las tecnologías de la información y a la vista de los progresos en la sociedad de la información.

Artículo 98. *Revisión de otros actos jurídicos de la Unión en materia de protección de datos.*

La Comisión presentará, si procede, propuestas legislativas para modificar otros actos jurídicos de la Unión en materia de protección de datos personales, a fin de garantizar la protección uniforme y coherente de las personas físicas en relación con el tratamiento. Se tratará en particular de las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento por parte de las instituciones, órganos, y organismos de la Unión y a la libre circulación de tales datos.

Artículo 99. *Entrada en vigor y aplicación.*

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea.

2. Será aplicable a partir del 25 de mayo de 2018.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

§ 8

Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos

Jefatura del Estado
«BOE» núm. 183, de 30 de julio de 2018
Última modificación: sin modificaciones
Referencia: BOE-A-2018-10751

I

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), es plenamente aplicable en España desde el pasado 25 de mayo.

El Reglamento General de Protección de Datos supone una profunda modificación del régimen vigente en materia de protección de datos personales, no sólo desde el punto de vista sustantivo y de cumplimiento por los sujetos obligados, sino particularmente en lo que afecta a la actividad de supervisión por parte de las autoridades de control que el mismo regula.

Además, la plena aplicación del Reglamento General de Protección de Datos implica que hayan de considerarse desplazadas por él aquellas disposiciones de Derecho interno que no resulten conformes con el régimen que el mismo establece. Así sucedería con muchos de los preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Por otra parte, numerosos preceptos del reglamento europeo se remiten a su desarrollo, obligatorio o potestativo, por los Estados miembros, conteniendo un total de cincuenta y seis remisiones a los ordenamientos nacionales. De entre estas remisiones, el reglamento impone a los Estados miembros, entre otras cuestiones, la regulación del estatuto de las autoridades de control, la determinación del régimen aplicable a los inspectores de un tercer Estado que lleven a cabo actividades conjuntas de investigación o la designación de la autoridad que representará al Estado miembro en el Comité Europeo de Protección de Datos.

Otras disposiciones del Reglamento General de Protección de Datos exigen una adecuación del Derecho interno, aun cuando no exista una remisión directa y expresa al mismo. Así, si bien el reglamento europeo establece un régimen sancionador en que se tipifican las conductas típicas, no regula cuestiones tan esenciales como los plazos de prescripción de dichas infracciones, al considerar que dicha cuestión corresponde al

ordenamiento de los Estados Miembros. Del mismo modo, establece un procedimiento de cooperación entre los Estados miembros en los supuestos de tratamientos denominados transfronterizos, con la participación de todas las autoridades implicadas, pero no regula el modo en que el Derecho interno de los Estados habrá de verse afectado como consecuencia de los trámites previstos en la propia norma europea para estos procedimientos.

La necesidad de adaptar el marco normativo interno al Reglamento General de Protección de Datos supuso la aprobación por el Consejo de Ministros en su sesión de 10 de noviembre de 2017 de un proyecto de ley orgánica, remitido a las Cortes Generales, que actualmente se encuentra en tramitación parlamentaria.

Teniendo en cuenta lo anterior, y sin perjuicio de que los aspectos que configuran el contenido esencial del derecho fundamental a la protección de datos de carácter personal hayan de incorporarse a una ley orgánica, no es menos cierto que en determinadas cuestiones que no son objeto de reserva de ley orgánica resulta imprescindible la adopción urgente de una norma con rango de ley que permita la adaptación del Derecho español al Reglamento General de Protección de Datos. En otras palabras, el objeto de este real decreto-ley se ciñe a la adecuación de nuestro ordenamiento al reglamento europeo en aquellos aspectos concretos que, sin rango orgánico, no admiten demora y debe entenderse sin perjuicio de la necesidad de una legislación orgánica de protección de datos que procure la plena adaptación de la normativa interna a los estándares fijados en la materia por la Unión Europea a través de una disposición directamente aplicable.

II

El real decreto-ley comprende catorce artículos estructurados en tres capítulos, dos disposiciones adicionales, dos transitorias, una derogatoria y una final. Su contenido afecta únicamente a cuestiones cuya inmediata incorporación al Derecho interno resulta imprescindible para la adecuada aplicación en España del Reglamento General de Protección de Datos y que no están excluidas del ámbito del legislador de urgencia por el artículo 86 de la Constitución Española.

El Capítulo I atiende a la necesidad de identificar al personal competente para el ejercicio de los poderes de investigación que el Reglamento General de Protección de Datos otorga en su artículo 58.1 a las autoridades de control. Ello exige que el Derecho interno regule el modo en que podrán ejercerse dichos poderes, qué personas ejercerán la actividad de investigación e inspección y en qué consistirán esas atribuciones expresamente establecidas en el reglamento europeo desde el punto de vista del ordenamiento español. Asimismo, y en aplicación del artículo 62.3 del Reglamento General de Protección de Datos, es preciso determinar el régimen aplicable al personal de las autoridades de supervisión de otros Estados miembros que participen en actuaciones conjuntas de investigación.

El Capítulo II articula el novedoso régimen sancionador establecido en el Reglamento General de Protección de Datos, reemplazando los tipos infractores actualmente contenidos en la Ley Orgánica 15/1999 por la remisión a los que están establecidos en los apartados 4, 5 y 6 del artículo 83 de dicho reglamento, lo que resulta de todo punto necesario. Además, existen dos cuestiones sobre las que es ineludible la adopción de disposiciones por el Derecho interno que garanticen la efectividad de este régimen sancionador y la seguridad jurídica en su aplicación. La primera se refiere a la necesaria delimitación de los sujetos que pudieran incurrir en la responsabilidad derivada de la aplicación de dicho régimen sancionador. La segunda reviste aún mayor importancia y se refiere a la necesidad de determinar los plazos de prescripción de las infracciones y sanciones previstas en la norma europea.

El Capítulo III contiene la regulación del procedimiento en caso de que exista una posible vulneración del Reglamento General de Protección de Datos. En este punto, es preciso tener en cuenta que el reglamento distingue en la práctica tres tipos de tratamientos a los que aplicaría distintas normas procedimentales: los tratamientos transfronterizos, definidos por el artículo 4.23 del Reglamento general de Protección de Datos, los transfronterizos con relevancia local en un Estado miembro, a los que se refiere el artículo 56 del mismo, y aquéllos que tendrían la condición de exclusivamente nacionales, entre los que figuran en todo caso los previstos en el artículo 55 de la norma europea. El reglamento europeo prevé una serie de trámites específicos para los dos primeros supuestos entre los que se

encuentran los necesarios para determinar la competencia de la autoridad de control principal, así como los que permiten la adopción de una decisión consensuada entre las autoridades principal e interesadas en el procedimiento. En estos casos la regulación europea establece la obligación de que la autoridad principal someta los distintos proyectos de decisión a las restantes autoridades, que dispondrán de plazos tasados para la emisión de «observaciones pertinentes motivadas», y previéndose el sometimiento de la resolución al Comité Europeo de Protección de Datos en caso de no alcanzarse un acuerdo entre todas ellas.

Estas previsiones han de trasladarse a la normas que regulen el procedimiento en caso de plantearse una reclamación ante la Agencia Española de Protección de Datos así como en los supuestos en que, sin haber recibido reclamación, tenga la condición de autoridad principal respecto de la reclamación recibida en otro Estado Miembros o considere que ha de intervenir como interesada en un procedimiento ya abierto.

Todo ello impone la necesidad de incorporar al procedimiento fases específicas como la admisión a trámite de las reclamaciones o la posibilidad de archivo provisional del expediente en los supuestos en que la Agencia Española de Protección de Datos no tramite la reclamación pero pueda tener que resolver sobre la misma. En particular, es indispensable incluir en las normas de procedimiento su suspensión en los supuestos en que proceda recabar el parecer de las autoridades de otros Estados miembros durante todo el tiempo previsto para su obtención, dado que en caso contrario existe una muy alta probabilidad de caducidad de los procedimientos, con las consecuencias negativas que ello conlleva no sólo para la aplicabilidad en España de las normas de protección de datos, sino para la garantía del derecho fundamental de los ciudadanos europeos en su conjunto en aquellos casos en que la Agencia Española de Protección de Datos tuviera la condición de autoridad de control principal.

En definitiva, este último capítulo tiene como objetivo hacer posible la aplicación de las especialidades del régimen procedimental del Reglamento General de Protección de Datos, en un contexto en el que, siendo la norma europea directamente aplicable, ya se han puesto en marcha procedimientos de especial trascendencia al amparo de este régimen.

Por último, en cumplimiento del artículo 68.4 del Reglamento General de Protección de Datos, la disposición adicional primera designa como representante de España en el Comité Europeo a la Agencia Española de Protección de Datos, que informará a las autoridades autonómicas acerca de las decisiones adoptadas en dicho organismo de la Unión y recabará su parecer cuando se trate de materias de su competencia. Por su parte, la disposición adicional segunda contiene previsiones en lo relativo a la publicidad de las resoluciones de la Agencia Española de Protección de Datos, con el fin de garantizar la transparencia de su actuación, ante el nuevo marco procedimental configurado por el Reglamento General de Protección de Datos.

En consecuencia, a la vista de los hechos descritos, la extraordinaria y urgente necesidad de este real decreto-ley resulta plenamente justificada. Dada la plena aplicación del Reglamento General de Protección de Datos desde el 25 de mayo de 2018, hasta la completa adecuación a él de nuestro ordenamiento, que solamente será posible a través de una nueva legislación orgánica, es ineludible la adopción de una disposición con rango de ley que permita la adaptación del Derecho español en varias cuestiones a la normativa de la Unión Europea en materia de protección de datos, para garantizar de forma efectiva el derecho del artículo 18.4 de la Constitución en un marco de seguridad jurídica. En coherencia con ello, la vigencia de este real decreto-ley se limita al período que medie entre el día siguiente de su publicación en el Boletín Oficial del Estado y la entrada en vigor de la nueva ley orgánica que se encuentra en tramitación parlamentaria.

Además, este real decreto-ley no afecta al ordenamiento de las instituciones básicas del Estado, a los derechos, deberes y libertades de los ciudadanos regulados en el Título I de la Constitución, al régimen de las Comunidades Autónomas ni al Derecho electoral general.

En definitiva, de todo lo anterior resulta que, en este caso, el real decreto-ley representa un instrumento constitucionalmente lícito, en tanto que pertinente y adecuado para la consecución del fin que justifica la legislación de urgencia, que no es otro, tal como reiteradamente ha exigido nuestro Tribunal Constitucional, que subvenir a un situación concreta, dentro de los objetivos gubernamentales, que por razones difíciles de prever

requiere una acción normativa inmediata en un plazo más breve que el requerido por la vía normal o por el procedimiento de urgencia para la tramitación parlamentaria de las Leyes.

Por tanto, en el conjunto y en cada una de las medidas que se adoptan, concurren, por su naturaleza y finalidad, las circunstancias de extraordinaria y urgente necesidad que exige el artículo 86 de la Constitución Española como presupuestos habilitantes para la aprobación de un real decreto-ley.

En su virtud, en uso de la autorización contenida en el artículo 86 de la Constitución Española, a propuesta de la Ministra de Justicia, previa deliberación del Consejo de Ministros en su reunión del día 27 de julio de 2018,

DISPONGO:

CAPÍTULO I

Inspección en materia de protección de datos

Artículo 1. *Ámbito y personal competente para el ejercicio de la actividad de investigación de la Agencia Española de Protección de Datos.*

1. La actividad de investigación de la Agencia Española de Protección de Datos se llevará a cabo por los funcionarios de la Agencia o por funcionarios ajenos a ella habilitados expresamente por su Director.

2. En los casos de actuaciones conjuntas de investigación conforme a lo dispuesto en el artículo 62 del Reglamento (UE) 2016/679, el personal de las autoridades de control de otros Estados Miembros de Unión Europea que colabore con la Agencia ejercerá sus facultades con arreglo a lo previsto en la normativa española y bajo la orientación y en presencia del personal de ésta.

3. Los funcionarios que desarrollen actividades de investigación tendrán la consideración de agentes de la autoridad en el ejercicio de sus funciones, y estarán obligados a guardar secreto sobre las informaciones que conozcan con ocasión de dicho ejercicio, incluso después de haber cesado en él.

Artículo 2. *Alcance de la actividad de investigación.*

Quienes desarrollen la actividad de investigación podrán recabar las informaciones precisas para el cumplimiento de sus funciones, realizar inspecciones, requerir la exhibición o el envío de los documentos y datos necesarios, examinarlos en el lugar en que se encuentren depositados o en donde se lleven a cabo los tratamientos, obtener copia de ellos, inspeccionar los equipos físicos y lógicos y requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del tratamiento sujetos a investigación. Los poderes de investigación en lo que se refiere a la entrada en domicilios deben ejercerse de conformidad con las normas procesales, en particular, en los casos en los que sea precisa la autorización judicial previa. Cuando se trate de órganos judiciales u Oficinas Judiciales el ejercicio de las facultades de inspección se efectuará a través y por mediación del Consejo General del Poder Judicial.

CAPÍTULO II

Régimen sancionador en materia de protección de datos

Artículo 3. *Sujetos responsables.*

1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y la normativa española de protección de datos:

a) Los responsables de los tratamientos.

b) Los encargados de los tratamientos.

c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.

d) Las entidades de certificación.
e) Las entidades acreditadas de supervisión de los códigos de conducta.

2. No será de aplicación al delegado de protección de datos el régimen sancionador en esta materia.

Artículo 4. *Infracciones.*

Constituyen infracciones las vulneraciones del Reglamento (UE) 2016/679 a las que se refieren los apartados 4, 5 y 6 de su artículo 83.

Artículo 5. *Prescripción de las infracciones.*

1. Las infracciones previstas en los apartados 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 prescribirán a los tres años.
2. Las infracciones previstas en el artículo 83.4 Reglamento (UE) 2016/679 prescribirán a los dos años.
3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.
Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679 interrumpirá la prescripción el conocimiento formal por el interesado del proyecto de acuerdo de inicio que sea sometido a las autoridades de control interesadas.

Artículo 6. *Prescripción de las sanciones.*

1. Las sanciones impuestas en aplicación del Reglamento (UE) 2016/679 prescriben en los siguientes plazos:

a) Las sanciones por importe igual o inferior a 40.000 euros, prescriben en el plazo de un año.
b) Las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años.
c) Las sanciones por un importe superior a 300.000 euros prescriben a los tres años.

2. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.
3. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

CAPÍTULO III

Procedimientos en caso de posible vulneración de la normativa de protección de datos

Artículo 7. *Régimen jurídico.*

1. Las disposiciones de este capítulo serán de aplicación a los procedimientos tramitados por la Agencia Española de Protección de Datos en los supuestos en los que un afectado reclame que no ha sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, así como en los que aquélla investigue la existencia de una posible infracción de lo dispuesto en el mencionado reglamento y la normativa española de protección de datos.
2. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la normativa española de

protección de datos y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos.

Artículo 8. *Forma de iniciación del procedimiento y duración.*

1. Cuando el procedimiento se refiera exclusivamente a la falta de atención de una solicitud de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, se iniciará por acuerdo de admisión a trámite, que se adoptará conforme a lo establecido en el artículo siguiente.

En este caso el plazo para resolver el procedimiento será de seis meses a contar desde la fecha en que hubiera sido notificado al reclamante el acuerdo de admisión a trámite. Transcurrido ese plazo, el interesado podrá considerar estimada su reclamación.

2. Cuando el procedimiento tenga por objeto la determinación de la posible existencia de una infracción de lo dispuesto en el Reglamento (UE) 2016/679 y la normativa española de protección de datos, se iniciará mediante acuerdo de inicio adoptado por propia iniciativa o como consecuencia de reclamación.

Si el procedimiento se fundase en una reclamación formulada ante la Agencia Española de Protección de Datos, con carácter previo, ésta decidirá sobre su admisión a trámite, conforme a lo dispuesto en el artículo siguiente.

Cuando fuesen de aplicación las normas establecidas en el artículo 60 del Reglamento (UE) 2016/679, el procedimiento se iniciará mediante la adopción del proyecto de acuerdo de inicio de procedimiento sancionador, del que se dará conocimiento formal al interesado a los efectos previstos en el artículo 5 de este real decreto-ley.

Admitida a trámite la reclamación así como en los supuestos en que la Agencia Española de Protección de Datos actúe por propia iniciativa, con carácter previo al acuerdo de inicio, podrá existir una fase de actuaciones previas de investigación, que se regirá por lo previsto en el artículo 11 de este real decreto-ley.

El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de inicio o, en su caso, del proyecto de acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad, y en consecuencia, el archivo de actuaciones.

3. El procedimiento podrá también tramitarse como consecuencia de la comunicación a la Agencia Española de Protección de Datos por parte de la autoridad de control de otro Estado miembro de la Unión Europea de la reclamación formulada ante la misma, cuando la Agencia Española de Protección de Datos tuviese la condición de autoridad de control principal para la tramitación de un procedimiento conforme a lo dispuesto en los artículos 56 y 60 del Reglamento (UE) 2016/679. Será en este caso de aplicación lo dispuesto en el apartado 1 y en los párrafos primero, tercero, cuarto y quinto del apartado 2.

4. Los plazos de tramitación establecidos en este artículo así como los de admisión a trámite regulado por el apartado 5 del artículo siguiente y de duración de las actuaciones previas de investigación previsto en el artículo 11.2 de este real decreto-ley, quedarán automáticamente suspendidos cuando deba recabarse información, consulta, solicitud de asistencia o pronunciamiento preceptivo de un órgano u organismo de la Unión Europea o de una o varias autoridades de control de los Estados miembros conforme con lo establecido en el Reglamento (UE) 2016/679, por el tiempo que medie entre la solicitud y la notificación del pronunciamiento a la Agencia Española de Protección de Datos.

Artículo 9. *Admisión a trámite de las reclamaciones.*

1. Cuando se presentase ante la Agencia Española de Protección de datos una reclamación, ésta deberá evaluar su admisibilidad a trámite, de conformidad con las previsiones de este artículo.

2. La Agencia Española de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos de carácter personal, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción.

3. Igualmente, la Agencia Española de Protección de Datos podrá inadmitir la reclamación cuando el responsable o encargado del tratamiento, previa advertencia formulada por la Agencia, hubiera adoptado las medidas correctivas encaminadas a poner

fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias:

a) Que no se haya causado perjuicio al afectado.

b) Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas.

4. Antes de resolver sobre la admisión a trámite de la reclamación, la Agencia Española de Protección de Datos podrá remitir la misma al delegado de protección de datos que hubiera, en su caso, designado el responsable o encargado del tratamiento o al organismo de supervisión establecido para la aplicación de los códigos de conducta, a fin de que den respuesta a la reclamación en el plazo de un mes.

La Agencia Española de Protección de Datos podrá igualmente remitir la reclamación al responsable o encargado del tratamiento cuando no se hubiera designado un delegado de protección de datos ni estuviera adherido a mecanismos de resolución extrajudicial de conflictos, en cuyo caso el responsable o encargado deberá dar respuesta a la reclamación también en el plazo de un mes.

5. La decisión sobre la admisión o inadmisión a trámite, así como la que determine, en su caso, la remisión de la reclamación a la Autoridad de control principal que se estime competente, deberá notificarse al reclamante en el plazo de tres meses. Si, transcurrido este plazo, no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación con arreglo a lo dispuesto en este capítulo a partir de la fecha en que se cumpliesen tres meses desde que la reclamación tuvo entrada en la Agencia Española de Protección de Datos.

Artículo 10. *Determinación del alcance territorial.*

1. Salvo en los supuestos a los que se refiere el artículo 8.3 de este real decreto-ley, la Agencia Española de Protección de Datos deberá, con carácter previo a la realización de cualquier otra actuación, incluida la admisión a trámite de una reclamación o el comienzo de actuaciones previas de investigación, examinar su competencia y determinar el carácter nacional o transfronterizo, en cualquiera de sus modalidades, del procedimiento a seguir.

2. Si la Agencia considera que no tiene la condición de autoridad de control principal para la tramitación del procedimiento remitirá, sin más trámite, la reclamación formulada a la Autoridad de control principal que considere competente, a fin de que por la misma se le dé el curso oportuno. La Agencia notificará esta circunstancia a quien, en su caso, hubiera formulado la reclamación.

El acuerdo por el que se resuelva la remisión a la que se refiere el párrafo anterior implicará el archivo provisional del procedimiento, sin perjuicio de que por la Agencia se dicte, en caso de que así proceda, la resolución a la que se refiere el apartado 8 del artículo 60 del Reglamento (UE) 2016/679.

Artículo 11. *Actuaciones previas de investigación.*

1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.

La Agencia Española de Protección de Datos actuará en todo caso cuando sea precisa la investigación de tratamientos que implique un tratamiento masivo de datos personales.

2. Las actuaciones previas de investigación se someterán a lo dispuesto en el capítulo I y no podrán tener una duración superior a doce meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha del acuerdo por el que se decida su iniciación cuando la Agencia actúe por propia iniciativa o como consecuencia de la comunicación que le hubiera sido remitida por la autoridad de control de otro Estado miembro de la Unión Europea, conforme al artículo 8.3 de este real decreto-ley.

Artículo 12. *Acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora.*

1. Concluidas, en su caso, las actuaciones a las que se refiere el artículo anterior, corresponderá al Director de la Agencia Española de Protección de Datos, cuando así proceda, dictar acuerdo de inicio de procedimiento para el ejercicio de la potestad sancionadora, en que se concretarán los hechos, la identificación de la persona o entidad contra la que se dirija el procedimiento, la infracción que hubiera podido cometerse y su posible sanción.

2. Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679, el proyecto de acuerdo de inicio de procedimiento sancionador se someterá a lo dispuesto en el mismo.

Artículo 13. *Medidas provisionales.*

1. Durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia Española de Protección de Datos podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos y, en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado.

2. En los casos en que la Agencia Española de Protección de Datos considere que la continuación del tratamiento de los datos de carácter personal, su comunicación o transferencia internacional comportara un menoscabo grave del derecho a la protección de datos de carácter personal, podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, caso de incumplirse por éstos dichos mandatos, proceder a su inmovilización.

3. Cuando se hubiese presentado ante la Agencia Española de Protección de Datos una reclamación que se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, la Agencia Española de Protección de Datos podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento para el ejercicio de la potestad sancionadora, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado, prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación.

Artículo 14. *Procedimiento en relación con las competencias atribuidas a la Agencia Española de Protección de Datos por otras leyes.*

Lo dispuesto en este capítulo será de aplicación a los procedimientos que la Agencia Española de Protección de Datos hubiera de tramitar en ejercicio de las competencias que le fueran atribuidas por otras leyes.

Disposición adicional primera. *Representación española en el Comité Europeo de Protección de Datos.*

La Agencia Española de Protección de Datos tendrá la condición de representante común de las autoridades de protección de datos en el Comité Europeo de Protección de Datos.

La Agencia Española de Protección de Datos informará a las autoridades autonómicas de protección de datos acerca de las decisiones adoptadas en el Comité Europeo de Protección de Datos y recabará su parecer cuando se trate de materias de su competencia.

Disposición adicional segunda. *Publicación de resoluciones de la Agencia Española de Protección de Datos.*

La Agencia Española de Protección de Datos publicará las resoluciones de su Director que declaren haber lugar o no a la atención de los derechos reconocidos en los artículos 15

a 22 del Reglamento (UE) 2016/679, las que pongan fin a los procedimientos de reclamación, las que archiven las actuaciones previas de investigación, las que sancionen con apercibimiento a las entidades a que se refiere el artículo 46 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, las que impongan medidas cautelares y las demás que disponga su Estatuto.

Disposición transitoria primera. *Régimen transitorio de los procedimientos.*

1. Los procedimientos ya iniciados a la entrada en vigor de este real decreto-ley se regirán por la normativa anterior, salvo que el régimen establecido en el mismo contenga disposiciones más favorables para el interesado.

2. Lo dispuesto en el apartado anterior será asimismo de aplicación a los procedimientos respecto de los cuales ya se hubieren iniciado las actuaciones previas a las que se refiere la Sección 2.ª del Capítulo III del Título IX del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Disposición transitoria segunda. *Contratos de encargado del tratamiento.*

Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas todas las normas de igual o inferior rango que se opongan a lo establecido en el presente real decreto-ley, y en particular, los siguientes artículos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal:

a) El artículo 40.
b) Los artículos 43 al 49, con excepción del artículo 46.

Disposición final única. *Vigencia.*

El presente real decreto-ley entrará en vigor al día siguiente de su publicación en el «Boletín Oficial del Estado» y lo estará hasta la vigencia de la nueva legislación orgánica de protección de datos que tenga por objeto adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.

§ 9

Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos

Ministerio de Relaciones con las Cortes y de la Secretaría del Gobierno
«BOE» núm. 106, de 4 de mayo de 1993
Última modificación: 5 de noviembre de 2008
Referencia: BOE-A-1993-11252

El título VI de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, ha configurado la Agencia de Protección de Datos como el ente independiente que debe garantizar el cumplimiento de las previsiones y mandatos en ella establecidos.

Algunos aspectos de dicho ente han sido objeto de regulación en la propia Ley que, no obstante, no ha agotado la materia y ha encomendado al Gobierno la regulación de la estructura orgánica y la aprobación del Estatuto de la Agencia de Protección de Datos.

Por medio de la presente disposición se procede a cumplimentar el doble mandato integrando la estructura del ente en su Estatuto propio.

En su virtud, a propuesta de los Ministros de Justicia y para las Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 26 de marzo de 1993,

D I S P O N G O :

Artículo único.

De conformidad con lo dispuesto en el artículo 34.2 y en la disposición final primera de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, se aprueba el Estatuto de la Agencia de Protección de Datos, cuyo texto se inserta a continuación.

Disposición adicional única.

Por el Ministerio de Economía y Hacienda se habilitarán los créditos necesarios para la instalación y funcionamiento de la Agencia de Protección de Datos, en tanto no sea aprobado el primer presupuesto de gastos e ingresos de la misma.

Disposición final única.

El presente Real Decreto entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

ESTATUTO DE LA AGENCIA DE PROTECCIÓN DE DATOS

CAPÍTULO I

Disposiciones generales

Artículo 1. *La Agencia de Protección de Datos.*

1. La Agencia de Protección de Datos es un ente de Derecho público de los previstos en el artículo 6, apartado 5, del texto refundido de la Ley General Presupuestaria, aprobado por Real Decreto legislativo 1091/1988, de 23 de septiembre, que tiene por objeto la garantía del cumplimiento y aplicación de las previsiones contenidas en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

2. La Agencia de Protección de Datos actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia.

Artículo 2. *Régimen jurídico.*

1. La Agencia de Protección de Datos goza de personalidad jurídica propia y plena capacidad pública y privada.

2. La Agencia de Protección de Datos se regirá por las disposiciones legales y reglamentarias siguientes:

a) El título VI de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

b) El presente Estatuto y las demás disposiciones de desarrollo de la Ley Orgánica 5/1992.

c) En defecto de las anteriores, y para el ejercicio de sus funciones públicas, las normas de procedimiento contenidas en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

d) Los preceptos de la Ley General Presupuestaria, texto refundido aprobado por Real Decreto legislativo 1091/1988, de 23 de septiembre, que resulten de aplicación.

e) Cuantas otras disposiciones resulten de aplicación.

3. La Agencia ejercerá sus funciones por medio del Director, a cuyo efecto los actos del Director se consideran actos de la Agencia.

4. Los actos dictados por el Director en el ejercicio de las funciones públicas de la Agencia agotan la vía administrativa. Contra ellos se podrán interponer los recursos contencioso-administrativos que resulten procedentes.

CAPÍTULO II

Funciones de la Agencia de Protección de Datos

Artículo 3. *Funciones.*

1. Corresponde a la Agencia de Protección de Datos ejercer las funciones que le atribuye el artículo 36 de la Ley Orgánica 5/1992.

2. A este efecto la Agencia de Protección de Datos podrá dirigirse directamente a los titulares y responsables de cualesquiera ficheros de datos de carácter personal.

Artículo 4. *Relaciones con los afectados.*

1. La Agencia de Protección de Datos informará a las personas de los derechos que la Ley les reconoce en relación con el tratamiento automatizado de sus datos de carácter personal y a tal efecto podrá promover campañas de difusión, valiéndose de los medios de comunicación social.

2. La Agencia atenderá las peticiones que le dirijan los afectados y resolverá las reclamaciones formuladas por los mismos, sin perjuicio de las vías de recurso procedentes.

Artículo 5. *Cooperación en la elaboración y aplicación de las normas.*

La Agencia de Protección de Datos colaborará con los órganos competentes en lo que respecta al desarrollo normativo y aplicación de las normas que incidan en materia propia de la Ley Orgánica 5/1992, y a tal efecto:

a) Informará preceptivamente los proyectos de disposiciones generales de desarrollo de la Ley Orgánica.
b) Informará preceptivamente cualesquiera proyectos de ley o reglamento que incidan en la materia propia de la Ley Orgánica.
c) Dictará instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica.
d) Dictará recomendaciones de aplicación de las disposiciones legales y reglamentarias en materia de seguridad de los datos y control de acceso a los ficheros.

Artículo 6. *Ficheros estadísticos.*

La Agencia de Protección de Datos ejercerá el control de la observancia de lo dispuesto en los artículos 4, 7 y 10 a 22 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, y en especial:

a) Informará con carácter preceptivo el contenido y formato de los cuestionarios, hojas censuales y otros documentos de recogida de datos con fines estadísticos.
b) Dictaminará sobre los procesos de recogida y tratamiento automatizado de los datos personales a efectos estadísticos.
c) Informará sobre los proyectos de ley por los que se exijan datos con carácter obligatorio y su adecuación a lo dispuesto en el artículo 7 de la Ley de la Función Estadística Pública.
d) Dictaminará sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos.

Artículo 7. *Publicidad de los ficheros automatizados.*

La Agencia de Protección de Datos velará por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, a cuyo efecto publicará y difundirá un catálogo anual de los ficheros inscritos en el Registro General de Protección de Datos, con expresión de la información que al amparo de lo dispuesto en el artículo 36, j), de la Ley Orgánica 5/1992, determine el Director.

Artículo 8. *Memoria anual.*

1. La Agencia de Protección de Datos redactará una Memoria anual sobre la aplicación de la Ley Orgánica 5/1992, y de las demás disposiciones legales y reglamentarias sobre protección de datos, la cual comprenderá, además de la información necesaria sobre el funcionamiento de la Agencia:

a) Una relación de los códigos tipo depositados e inscritos en el Registro General de Protección de Datos.
b) Un análisis de las tendencias legislativas, jurisprudenciales y doctrinales de los distintos países en materia de protección de datos.
c) Un análisis y una valoración de los problemas de la protección de datos a escala nacional.

2. La Memoria anual será remitida por el Director al Ministro de Justicia, para su ulterior envío a las Cortes Generales.

Artículo 9. *Relaciones internacionales.*

1. Corresponde a la Agencia de Protección de Datos la cooperación con organismos internacionales y órganos de las Comunidades Europeas en materia de protección de datos.

2. La Agencia prestará asistencia a las autoridades designadas por los Estados parte en el Convenio del Consejo de Europa de 28 de enero de 1981, sobre protección de las personas en relación con el tratamiento automatizado de los datos de carácter personal, a los efectos previstos en el artículo 13 del Convenio.

3. Se designa a la Agencia de Protección de Datos como representante español a los efectos previstos en el artículo 29 de la Directiva 95/46/CE, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Corresponde al Director de la Agencia la designación de un representante para el Grupo de Protección de las Personas en lo que respecta al tratamiento de datos personales, previsto en la disposición citada.

Artículo 10. *Sistema de Información Schengen.*

1. La Agencia de Protección de Datos ejercerá el control de los datos de carácter personal introducidos en la parte nacional española de la base de datos del Sistema de Información Schengen (SIS).

2. El Director de la Agencia designará dos representantes para la autoridad de control común de protección de datos del Sistema de Información Schengen.

CAPÍTULO III

Organos de la Agencia de Protección de Datos

Sección 1. Estructura orgánica de la Agencia de Protección de Datos

Artículo 11. *Estructura orgánica.*

La Agencia de Protección de Datos se estructura en los siguientes órganos:

1. El Director de la Agencia de Protección de Datos.
2. El Consejo Consultivo.
3. El Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General, como órganos jerárquicamente dependientes del Director de la Agencia.

Sección 2. El Director de la Agencia de Protección de Datos

Artículo 12. *Funciones de dirección.*

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación.

2. Corresponde al Director de la Agencia de Protección de Datos dictar las resoluciones e instrucciones que requiera el ejercicio de las funciones de la Agencia y, en especial:

a) Resolver motivadamente sobre la procedencia o improcedencia de las inscripciones que deban practicarse en el Registro General de Protección de Datos.

b) Requerir a los responsables de ficheros de titularidad privada a que subsanen deficiencias de los códigos tipo.

c) Resolver motivadamente, previo informe del responsable del fichero, sobre la procedencia o improcedencia de la denegación, total o parcial, del acceso a los ficheros policiales o tributarios automatizados.

d) Autorizar transferencias temporales o definitivas de datos que hayan sido objeto de tratamiento automatizado o recogidos a tal efecto, con destino a países cuya legislación no ofrezca un nivel de protección equiparable al de la Ley Orgánica 5/1992 y el presente estatuto.

e) Convocar regularmente a los órganos competentes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación.

f) Recabar de las distintas Administraciones Públicas la información necesaria para el cumplimiento de sus funciones.

g) Solicitar de los órganos correspondientes de las Comunidades Autónomas, a que se refiere el artículo 40 de la Ley Orgánica 5/1992, la información necesaria para el cumplimiento de sus funciones, así como facilitar a aquéllos la información que le soliciten a idénticos efectos.

h) Adoptar las medidas cautelares y provisionales que requiera el ejercicio de la potestad sancionadora de la Agencia con relación a los responsables de los ficheros privados.

i) Iniciar, impulsar la instrucción y resolver los expedientes sancionadores referentes a los responsables de los ficheros privados.

j) Instar la incoación de expedientes disciplinarios en los casos de infracciones cometidas por órganos responsables de ficheros de las Administraciones Públicas.

k) Autorizar la entrada en los locales en los que se hallen los ficheros, con el fin de proceder a las inspecciones pertinentes, sin perjuicio de la aplicación de las reglas que garantizan la inviolabilidad del domicilio.

Artículo 13. *Funciones de gestión.*

1. Corresponde asimismo al Director de la Agencia de Protección de Datos:

a) Adjudicar y formalizar los contratos que requiera la gestión de la Agencia y vigilar su cumplimiento y ejecución.

b) Aprobar gastos y ordenar pagos, dentro de los límites de los créditos del presupuesto de gastos de la Agencia.

c) Ejercer el control económico-financiero de la Agencia.

d) Programar la gestión de la Agencia.

e) Elaborar el anteproyecto de presupuesto de la Agencia.

f) Proponer la relación de puestos de trabajo de la Agencia.

g) Aprobar la Memoria anual de la Agencia.

h) Ordenar la convocatoria de las reuniones del Consejo Consultivo.

2. El Director podrá delegar en el Secretario general el ejercicio de las funciones a que se refieren las letras a), b), d), e) y f) del apartado anterior.

Artículo 13 bis. *Régimen de suplencia.*

1. En los supuestos de ausencia, vacante o enfermedad del Director de la Agencia Española de Protección de Datos, el ejercicio de las competencias previstas en los artículos 12.2 y 13.1 del presente Estatuto, así como las que le correspondieran en aplicación de lo previsto en el artículo 37 de la Ley Orgánica 5/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, será asumido por el Subdirector General de la Inspección de Datos. En el supuesto de que cualquiera de las circunstancias mencionadas concurriera igualmente en él, el ejercicio de las competencias afectadas será asumido por el Subdirector General del Registro General de Protección de Datos y, en su defecto, por el Secretario General.

2. Cuando, conforme a lo previsto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, concurriera en el Director de la Agencia Española de Protección de Datos alguna causa de abstención o recusación, el ejercicio de las competencias a las que se refiere el apartado anterior, será asumido por el Subdirector General de la Inspección de Datos. En el supuesto de que cualquiera de las causas mencionadas concurriera igualmente en él, el ejercicio de las competencias afectadas será asumido por el Subdirector General del Registro General de Protección de Datos y, en su defecto, por el Secretario General.

Artículo 14. *Nombramiento y mandato.*

1. El Director de la Agencia de Protección de Datos será nombrado por el Gobierno, mediante Real Decreto, a propuesta del Ministro de Justicia, de entre los miembros del Consejo Consultivo.

2. El Director de la Agencia de Protección de Datos gozará de los mismos honores y tratamiento que los Subsecretarios.

3. El mandato del Director de la Agencia de Protección de Datos tendrá una duración de cuatro años contados desde su nombramiento y sólo cesará por las causas previstas en el artículo 15 del presente Estatuto.

Artículo 15. *Cese y separación.*

1. El Director de la Agencia de Protección de Datos cesará en el desempeño de su cargo por la expiración de su mandado o, con anterioridad, a petición propia.

2. El Gobierno sólo podrá acordar la separación del Director de la Agencia de Protección de Datos antes de que hubiera expirado el plazo de su mandato en los casos siguientes:

a) Incumplimiento grave de las obligaciones del cargo.
b) Incapacidad sobrevenida para el ejercicio de sus funciones.
c) Incompatibilidad.
d) Condena por delito doloso.

La separación se acordará por el Gobierno, mediante Real Decreto a propuesta del Ministro de Justicia, previa instrucción de expediente, en el cual serán oídos los restantes miembros del Consejo Consultivo.

3. El cargo de Director de la Agencia de Protección de Datos está sujeto a las incompatibilidades que para los altos cargos prevé la Ley 25/1983, de 26 de diciembre.

Artículo 16. *Independencia.*

1. El Director de la Agencia de Protección de Datos desempeñará su cargo con dedicación absoluta, plena independencia y total objetividad.

2. El Director no estará sujeto a mandato imperativo, ni recibirá instrucciones de autoridad alguna.

Artículo 17. *Remuneración.*

1. El Director de la Agencia de Protección de Datos percibirá la remuneración que en los Presupuestos Generales del Estado tengan asignada los subsecretarios.

2. La remuneración será incompatible con la percepción de pensiones de derechos pasivos o de cualquier régimen de Seguridad Social público y obligatorio, quedando en suspenso dichas percepciones durante el plazo de mandato.

Sección 3. El Consejo Consultivo

Artículo 18. *El Consejo Consultivo.*

1. El Consejo Consultivo de la Agencia de Protección de Datos, establecido por el artículo 37 de la Ley Orgánica 5/1992, de 29 de octubre, es un órgano colegiado de asesoramiento del Director de la Agencia de Protección de Datos.

2. El Consejo Consultivo emitirá informe en todas las cuestiones que le someta el Director de la Agencia de Protección de Datos y podrá formular propuestas en temas relacionados con las materias de competencia de ésta.

Artículo 19. *Propuesta y nombramiento.*

1. Los miembros del Consejo Consultivo serán propuestos en la forma siguiente:

a) El Congreso de los Diputados propondrá, como Vocal, a un Diputado.
b) El Senado propondrá, como Vocal, a un Senador.

c) El Ministro de Justicia propondrá al Vocal de la Administración General del Estado.

d) Las Comunidades Autónomas decidirán, mediante acuerdo adoptado por mayoría simple, el Vocal a proponer.

e) La Federación Española de Municipios y Provincias propondrá al Vocal de la Administración Local.

f) La Real Academia de la Historia propondrá, como Vocal, a un miembro de la Corporación.

g) El Consejo de Universidades propondrá a un Vocal experto en la materia de entre los cuerpos docentes de enseñanza superior e investigadores con acreditado conocimiento en el tratamiento automatizado de datos.

h) El Consejo de Consumidores y Usuarios propondrá, mediante terna, al Vocal de los usuarios y consumidores.

i) El Consejo Superior de Cámaras de Comercio, Industria y Navegación propondrá, mediante terna, al Vocal del sector de ficheros privados.

2. Las propuestas serán elevadas al Gobierno por conducto del Ministro de Justicia.

3. Los miembros del Consejo Consultivo serán nombrados y, en su caso, cesados por el Gobierno.

Artículo 20. *Plazo y vacantes.*

1. Los miembros del Consejo Consultivo desempeñarán su cargo durante cuatro años.

2. Se exceptúan de lo establecido en el apartado anterior los siguientes supuestos:

a) Nombramiento del Vocal como Director de la Agencia de Protección de Datos.

b) Renuncia anticipada del Vocal.

c) Pérdida de la condición que habilitó al Vocal para ser propuesto, en los supuestos previstos en las letras a), b), f) y g) del apartado 1 del artículo anterior.

d) Propuesta de cese emanada de las instituciones, órganos, corporaciones u organizaciones a las que se refiere el artículo anterior.

3. Las vacantes que se produzcan en el Consejo Consultivo antes de expirar el plazo a que se refiere el apartado 1 deberán ser cubiertas dentro del mes siguiente a la fecha en que la vacante se hubiera producido, por el procedimiento previsto en el artículo anterior y por el tiempo que reste para completar el mandato de quien causó la vacante a cubrir.

4. Los miembros del Consejo Consultivo no percibirán retribución alguna, sin perjuicio del abono de los gastos, debidamente justificados, que les ocasione el ejercicio de su función.

Artículo 21. *Renovación del Consejo Consultivo.*

1. Antes de finalizar el mandato de los miembros del Consejo Consultivo, el Gobierno, por conducto del Ministro de Justicia, requerirá a las instituciones, órganos, corporaciones y organizaciones a que se refiere el artículo 19 del presente Estatuto, a fin de que le comuniquen los nombres de las personas que propongan para un nuevo mandato en el Consejo Consultivo, lo que deberá efectuarse dentro del mes siguiente a la formulación del referido requerimiento.

2. Una vez transcurrido el plazo señalado para cumplimentar el requerimiento, el Gobierno procederá, sin más trámites, a nombrar como miembros del Consejo Consultivo a los propuestos, quienes tomarán posesión de su condición en la misma fecha en que expire el anterior mandato de los miembros del Consejo.

Artículo 22. *Funcionamiento.*

1. En defecto de disposiciones específicas del presente Estatuto, el Consejo Consultivo ajustará su actuación, en lo que le sea de aplicación, a las disposiciones del capítulo II del título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. El Consejo Consultivo adoptará sus acuerdos en sesión plenaria.

3. Actuará como presidente del Consejo Consultivo el Director de la Agencia de Protección de Datos.

4. Actuará como secretario del Consejo Consultivo, con voz y sin voto, el titular de la Secretaría General de la Agencia de Protección de Datos. En caso de vacante, ausencia o enfermedad, actuará de secretario un funcionario adscrito a la Secretaría General designado por el Director de la Agencia a tal efecto.

5. El Consejo Consultivo se reunirá cuando así lo decida el Director de la Agencia que, en todo caso, lo convocará una vez cada seis meses. También se reunirá cuando así lo solicite la mayoría de sus miembros.

6. El Secretario convocará las reuniones del Consejo Consultivo, de orden del Director de la Agencia, y trasladará la convocatoria a los miembros del Consejo.

7. El Consejo Consultivo quedará válidamente constituido, en primera convocatoria, si están presentes el presidente, el secretario y la mitad de los miembros del Consejo, y, en segunda convocatoria, si están presentes el presidente, el secretario y la tercera parte de los miembros del Consejo.

Sección 4. El Registro General de Protección de Datos

Artículo 23. *El Registro General de Protección de Datos.*

El Registro General de Protección de Datos es el órgano de la Agencia de Protección de Datos al que corresponde velar por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos regulados en los artículos 13 a 15 de la Ley Orgánica 5/1992, de 29 de octubre.

Artículo 24. *Ficheros inscribibles.*

1. Serán objeto de inscripción en el Registro los ficheros automatizados que contengan datos personales y de los cuales sean titulares:

a) La Administración General del Estado.

b) Las entidades y organismos de la Seguridad Social.

c) Los organismos autónomos del Estado, cualquiera que sea su clasificación.

d) Las sociedades estatales y entes del sector público a que se refiere el artículo 6 de la Ley General Presupuestaria.

e) Las Administraciones de las Comunidades Autónomas y de sus Territorios Históricos, así como sus entes y organismos dependientes, sin perjuicio de que se inscriban además en los registros a que se refiere el artículo 40.2 de la Ley Orgánica 5/1992.

f) Las entidades que integran la Administración Local y los entes y organismos dependientes de la misma.

g) Cualesquiera otras personas jurídico-públicas, así como las personas privadas, físicas o jurídicas.

2. En los asientos de inscripción de los ficheros de titularidad pública figurará, en todo caso, la información contenida en la disposición general de creación o modificación del fichero, de conformidad con lo previsto en el artículo 18.2 de la Ley Orgánica 5/1992, de 29 de octubre.

3. En los asientos de inscripción de los ficheros de titularidad privada figurarán, en todo caso, la información contenida en la notificación del fichero a excepción de las medidas de seguridad, así como los cambios de finalidad del fichero, de responsable y de ubicación del fichero.

4. En los asientos de inscripción de cualesquiera ficheros de datos de carácter personal figurarán los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación y cancelación.

Artículo 25. *Actos y documentos inscribibles.*

Se inscribirán en el Registro General de Protección de Datos los siguientes actos y documentos:

a) Las autorizaciones de transferencia de datos personales a otros países, en los casos en que, a tenor de lo dispuesto en el artículo 32 de la Ley Orgánica 5/1992, de 29 de octubre, sea preceptiva para la transferencia la autorización previa del Director.

b) Los códigos tipo elaborados al amparo de lo previsto en el artículo 31 de la Ley Orgánica 5/1992.

Artículo 26. *Inscripción y certificaciones.*

1. Corresponde al Registro General de Protección de Datos instruir los expedientes de inscripción de los ficheros automatizados de titularidad privada y pública.

2. Corresponde asimismo al Registro General de Protección de Datos:

a) Instruir los expedientes de modificación y cancelación del contenido de los asientos.
b) Instruir los expedientes de autorización de las transferencias internacionales de datos.
c) Rectificar de oficio los errores materiales de los asientos.
d) Expedir certificaciones de los asientos.
e) Publicar una relación anual de los ficheros notificados e inscritos.

Sección 5. La Inspección de Datos

Artículo 27. *La Inspección de Datos.*

1. La Inspección de Datos es el órgano de la Agencia de Protección de Datos al cual competen las funciones inherentes al ejercicio de la potestad de inspección que el artículo 39 de la Ley Orgánica 5/1992, de 29 de octubre, atribuye a la Agencia.

2. Los funcionarios que ejerzan funciones inspectoras tendrán la consideración de autoridad pública en el desempeño de sus funciones, y estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 28. *Funciones inspectoras.*

1. Compete, en particular, a la Inspección de Datos efectuar inspecciones, periódicas o circunstanciales, de oficio o a instancia de los afectados, de cualesquiera ficheros, de titularidad pública o privada, en los locales en los que se hallen los ficheros y los equipos informáticos correspondientes, y a tal efecto podrá:

a) Examinar los soportes de información que contengan los datos personales.
b) Examinar los equipos físicos.
c) Requerir el pase de programas y examinar la documentación pertinente al objeto de determinar, en caso necesario, los algoritmos de los procesos de que los datos sean objeto.
d) Examinar los sistemas de transmisión y acceso a los datos.
e) Realizar auditorías de los sistemas informáticos con miras a determinar su conformidad con las disposiciones de la Ley Orgánica 5/1992.
f) Requerir la exhibición de cualesquiera otros documentos pertinentes.
g) Requerir el envío de toda información precisa para el ejercicio de las funciones inspectoras.

2. El responsable del fichero estará obligado a permitir el acceso a los locales en los que se hallen los ficheros y los equipos informáticos previa exhibición por el funcionario actuante de la autorización expedida por el Director de la Agencia. Cuando dichos locales tengan la consideración legal de domicilio, la labor inspectora deberá ajustarse además a las reglas que garantizan su inviolabilidad.

Artículo 29. *Funciones instructoras.*

Compete a la Inspección de Datos el ejercicio de los actos de instrucción relativos a los expedientes sancionadores a los que se refiere el artículo 12.2.h) del presente Estatuto.

Sección 6. La Secretaría General

Artículo 30. *Funciones de apoyo y ejecución.*

Corresponde a la Secretaría General:

a) Elaborar los informes y propuestas que le solicite el Director.
b) Notificar las resoluciones del Director.
c) Ejercer la Secretaría del Consejo Consultivo.
d) Gestionar los medios personales y materiales adscritos a la Agencia.
e) Atender a la gestión económico-administrativa del presupuesto de la Agencia.
f) Llevar el inventario de bienes y derechos que se integren en el patrimonio de la Agencia.
g) Gestionar los asuntos de carácter general no atribuidos a otros órganos de la Agencia.

Artículo 31. *Otras funciones.*

Corresponde asimismo a la Secretaría General:

a) Formar y actualizar un fondo de documentación sobre legislación, jurisprudencia y doctrina en materia de protección de datos personales y cualesquiera materias conexas.
b) Editar los repertorios oficiales de ficheros inscritos en el Registro General de Protección de Datos, las Memorias anuales de la Agencia y cualesquiera publicaciones de la Agencia.
c) Organizar conferencias, seminarios y cualesquiera actividades de cooperación internacional e interregional sobre protección de datos.
d) Facilitar la información a que se refiere el artículo 4.1 del presente Estatuto.

CAPITULO IV

Régimen económico, patrimonial y de personal

Sección 1. Régimen económico

Artículo 32. *Recursos económicos.*

Los recursos económicos de la Agencia de Protección de Datos comprenderán:

a) Las asignaciones que anualmente se establezcan con cargo a los Presupuestos Generales del Estado.
b) Las subvenciones y aportaciones que se concedan a su favor, procedentes de fondos específicos de la Comunidad Económica Europea.
c) Los ingresos, ordinarios y extraordinarios derivados del ejercicio de sus actividades.
d) Las rentas y productos de los bienes, derechos y valores integrantes de su patrimonio.
e) El producto de la enajenación de sus activos.
f) Cualesquiera otros que legalmente puedan serle atribuidos.

Artículo 33. *Contabilidad y control.*

1. La Agencia de Protección de Datos ajustará su contabilidad al Plan General de Contabilidad Pública y a las demás disposiciones que sean de aplicación, sin perjuicio de la obligación de rendir cuentas al Tribunal de Cuentas por conducto de la Intervención General de la Administración del Estado, en los términos previstos en la Ley General Presupuestaria.
2. El ejercicio anual se computará por años naturales, comenzando el día 1 del mes de enero de cada año.
3. El control de las actividades económicas y financieras de la Agencia se ejercerá de conformidad con lo establecido en el artículo 17.1 de la Ley General Presupuestaria, con carácter permanente.

Artículo 34. *Presupuestos.*

1. La Agencia de Protección de Datos elaborará anualmente un anteproyecto de presupuesto, con la estructura que señale el Ministerio de Economía y Hacienda, y lo remitirá a éste para su ulterior elevación al Gobierno a fin de que sea integrado con la debida independencia en los Presupuestos Generales del Estado.

2. Las modificaciones del presupuesto de la Agencia serán autorizadas por el Director cuando se trate de modificaciones internas que no incrementen la cuantía del mismo y sean consecuencia de las necesidades surgidas durante el ejercicio.

3. Los suplementos de crédito o créditos extraordinarios de la Agencia serán autorizados por el Ministro de Economía Hacienda cuando no excedan del 5 por 100 de su presupuesto de gastos y por el Gobierno en los demás casos.

Sección 2. Régimen patrimonial

Artículo 35. *Patrimonio.*

1. La Agencia de Protección de Datos tendrá un patrimonio propio, distinto del del Estado, formado por los bienes, derechos y valores que adquiera a título oneroso o le sean cedidos o donados por cualquier persona o entidad.

2. Los bienes que el Estado adscriba a la Agencia quedarán afectados a su servicio y conservarán la calificación jurídica originaria, debiendo ser utilizados exclusivamente para los fines que determinaron la adscripción.

Artículo 36. *Adquisiciones y contratación.*

1. La Agencia de Protección de Datos se regirá, en lo referente a las adquisiciones y enajenaciones de bienes, por las disposiciones del derecho privado.

2. Los bienes que adquiera la Agencia se integrarán en su patrimonio.

3. Los contratos que celebre la Agencia se regirán por las disposiciones del derecho privado, sin perjuicio de que la adjudicación de los contratos sea acordada previa publicidad y promoción de concurrencia.

Sección 3. Régimen del personal

Artículo 37. *Relación de puestos de trabajo.*

1. La Agencia de Protección de Datos propondrá a los órganos competentes, a través del Ministerio de Justicia, la relación de puestos de trabajo de la misma.

2. La relación de puestos de trabajo comprenderá:

a) Los puestos de trabajo a desempeñar por personal funcionario. Los titulares de los órganos a que se refiere el artículo 11.3 tendrán rango de Subdirector general.

b) Los puestos de trabajo a desempeñar por personal laboral, con expresión de los factores que, en función de las tareas integrantes de cada puesto de trabajo, determinen la imposibilidad de su desempeño por personal funcionario.

3. Las descripciones de los puestos de trabajo indicarán expresamente la obligación que, a tenor de lo previsto en los artículos 10 y 39 de la Ley Orgánica 5/1992, de 29 de octubre, corresponde al personal en lo relativo a la observancia de secreto sobre los datos personales, que los titulares de cada puesto conozcan en el desempeño de sus tareas.

Artículo 38. *Retribuciones.*

Las retribuciones del personal funcionario y laboral de la Agencia se ajustarán a lo dispuesto en las leyes anuales de presupuestos.

Artículo 39. *Provisión de puestos de trabajo.*

1. La Agencia de Protección de Datos proveerá los puestos de trabajo adscritos al personal funcionario ajustándose a la legislación de la Función Pública.

2. Los puestos de trabajo adscritos al personal laboral se proveerán mediante convocatoria pública y de acuerdo con los principios de igualdad, mérito y capacidad.

Disposición adicional primera. *Plazo para efectuar las propuestas de nombramiento.*

En el plazo de un mes a contar de la entrada en vigor del presente Estatuto, las instituciones, órganos, corporaciones y organizaciones a que se refiere el artículo 19 del mismo, comunicarán los nombres de las personas que deban proponer para su nombramiento como miembros del Consejo Consultivo.

Disposición adicional segunda. *Nombramiento de los miembros del Consejo Consultivo.*

Transcurrido el plazo establecido en la disposición adicional primera, el Gobierno nombrará sin más trámite a los miembros del Consejo Consultivo que hubieran sido propuestos y designará de entre ellos al Director de la Agencia.

Disposición adicional tercera. *Ficheros excluidos.*

1. En los términos y con los límites establecidos en los artículos 21.3 y 40 de la Ley Orgánica 5/1992, de 29 de octubre, quedan excluidos del ámbito de aplicación del presente Estatuto los ficheros automatizados de datos de carácter personal creados o gestionados por las Comunidades Autónomas.

2. Asimismo quedan excluidos del ámbito de aplicación del presente Estatuto los ficheros a los que se refiere el artículo 2, apartados 2 y 3, de la Ley Orgánica 5/1992, de 29 de octubre, salvo lo establecido en este último apartado para los ficheros que sirvan a fines exclusivamente estadísticos.

§ 10

Resolución de 24 de mayo de 2010, de la Agencia Española de Protección de Datos, por la que se regula el Registro Electrónico de la Agencia Española de Protección de Datos

Agencia Española de Protección de Datos
«BOE» núm. 135, de 3 de junio de 2010
Última modificación: sin modificaciones
Referencia: BOE-A-2010-8827

Las iniciativas de simplificación y modernización administrativa, que potencian el uso de medios electrónicos por parte de las Administraciones Públicas en sus relaciones con los ciudadanos han sido numerosas a lo largo de los últimos años.

En el marco de dichas iniciativas y por medio de Resolución de 12 de julio de 2006 se creó el Registro Telemático de la Agencia Española de Protección de Datos, encargado de la recepción y remisión de solicitudes, escritos y comunicaciones vinculadas al procedimiento de notificación de ficheros con datos de carácter personal para su inscripción en el Registro General de Protección de Datos mediante el formulario electrónico de Notificaciones Telemáticas a la AEPD (NOTA).

Posteriormente, la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, establece, en sus artículos 24, 25 y 26, una nueva regulación de los registros electrónicos, siendo sus preceptos desarrollados por el Título IV del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la citada Ley, que regula las condiciones de su funcionamiento.

El artículo 24.1 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, establece que las administraciones públicas crearán registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones.

Asimismo, el artículo 25.1 de la misma Ley prevé que las disposiciones de creación de registros electrónicos especificarán el órgano o unidad responsable de su gestión, así como la fecha y hora oficial y los días declarados como inhábiles a los efectos de cómputo de plazos. Con mayor detalle, el artículo 27 del Real Decreto 1671/2009 establece que los registros electrónicos serán creados, en el caso de Organismos Públicos, mediante Resolución de su titular, debiendo dicha Resolución respetar el contenido mínimo establecido en el apartado 2 de dicho precepto.

La disposición transitoria única de la Ley 11/2007, de 22 de junio, establece en su segundo párrafo que los registros telemáticos existentes a su entrada en vigor serán considerados registros electrónicos, regulándose por lo dispuesto en los mencionados artículos 24, 25 y 26. Este régimen resultaba ya, por tanto, de aplicación al Registro telemático de esta Agencia, creado por la ya citada Resolución de 12 de julio de 2006.

Sin embargo, el nuevo marco establecido por la Ley 11/2007 y su normativa de desarrollo y las consecuencias de la progresiva implantación y desarrollo de la Administración Electrónica, unido a las especialidades derivadas del nuevo régimen legal

creado por las citadas normas aconsejan la adopción de una nueva regulación del Registro Electrónico de la Agencia Española de Protección de Datos.

En este sentido, la disposición final tercera del Real Decreto 1671/2009, de 6 de noviembre, establece que los registros telemáticos ajustarán su funcionamiento a lo establecido en el mismo dentro de los seis meses siguientes a su entrada en vigor, lo que deberá verificarse, según establece esa disposición, mediante Orden Ministerial o, en su caso, Resolución del titular del correspondiente Organismo Público, que deberá explicitar el contenido previsto en el artículo 27 del Real Decreto.

En su virtud, dispongo:

Artículo 1. *Objeto.*

1. La presente Resolución tiene como objeto la regulación del Registro electrónico de la Agencia Española de Protección de Datos en adelante «Registro Electrónico», para la recepción y remisión, por vía electrónica, de solicitudes, escritos y comunicaciones en el ámbito de los procedimientos y actuaciones incluidos en el anexo I y en la forma prevista en el artículo 24 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la citada Ley.

2. El acceso de los interesados al Registro Electrónico estará disponible a través de la Sede Electrónica del Agencia Española de Protección de Datos en la dirección sedeagpd.gob.es y en la dirección electrónica www.agpd.es

3. El registro Electrónico será único para todos los órganos de la Agencia Española de Protección de Datos.

Artículo 2. *Ámbito del Registro Electrónico de la Agencia Española de Protección de Datos.*

1. El Registro Electrónico estará habilitado únicamente para la recepción y remisión de escritos, solicitudes y comunicaciones que se presenten por medios electrónicos respecto de los trámites y procedimientos incluidos en el anexo I de esta resolución o de la versión que figure actualizada en cada momento, en la dirección electrónica de acceso al mismo junto con los correspondientes modelos normalizados para cada caso.

2. Cualquier solicitud, escrito, comunicación o documentación presentada ante el Registro Electrónico no relacionada con los trámites y procedimientos a que se refiere el apartado anterior, será remitido a las personas, órganos o unidades destinatarias, en los términos previstos en el artículo 24.2.b) de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y en el Real Decreto 1671/2009, de 6 de noviembre, que desarrolla parcialmente la citada ley.

3. Asimismo, se podrá localizar un formulario genérico que permita la presentación de solicitudes, escritos y comunicaciones no asociados a procedimientos normalizados.

4. El Registro Electrónico podrá rechazar los documentos electrónicos que se encuentren en alguna de las circunstancias previstas en el artículo 29.1 del Real Decreto 1671/2009, de 6 de noviembre, en la forma establecida en el mismo. En su caso, la notificación al remitente se hará de conformidad con lo allí dispuesto.

Artículo 3. *Sistemas de identificación y autenticación.*

1. Las solicitudes, escritos y comunicaciones podrán ser presentados ante el Registro Electrónico por los interesados o sus representantes, en los términos definidos en los artículos 30 y siguientes de la Ley 30/1992, de 26 de noviembre.

2. El firmante del documento podrá acreditar su identidad ante el Registro Electrónico mediante firma electrónica o a través de funcionarios públicos habilitados, mediante el procedimiento previsto en el artículo 22 de la Ley 11/2007, de 22 de junio.

3. Adicionalmente, cuando estén operativos los respectivos sistemas, los documentos podrán ser presentados por representación, de acuerdo con lo dispuesto en el artículo 23 de la Ley 11/2007, de 22 de junio, y artículos 13 y 14 del Real Decreto 1671/2009, de 6 de noviembre.

4. La sede electrónica informará sobre los sistemas de representación y de autenticación y firma utilizables para la presentación de escritos ante el Registro Electrónico a través de

sus aplicaciones gestoras, con especificación, en su caso, de los servicios, procedimientos y trámites a los que sean de aplicación.

5. Cuando la representación no quede acreditada o no pueda presumirse, se requerirá dicha acreditación por la vía que corresponda.

6. Se admitirán los sistemas de firma electrónica que sean conformes con lo establecido en el artículo 10 del Real Decreto 1671/2009, de 6 de noviembre, por le que se desarrolla parcialmente la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos.

7. La identificación y firma de personas físicas mediante la utilización del documento nacional de identidad electrónico serán admitidas en todos los casos.

Artículo 4. *Voluntariedad de la presentación electrónica.*

La presentación de solicitudes, escritos y comunicaciones por medio del Registro Electrónico tendrá carácter voluntario, salvo lo previsto en el artículo 27.6 de la Ley 11/2007, de 22 de junio, siendo alternativa a la utilización de los lugares señalados en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de la Administraciones Pública y del Procedimiento Administrativo Común.

Artículo 5. *Presentación de documentos y computo de plazos.*

1. El Registro Electrónico permitirá la presentación de solicitudes, escritos y comunicaciones todos los días del año, durante las veinticuatro horas del día, sin perjuicio de las interrupciones, por el tiempo imprescindible cuando concurran razones justificadas de mantenimiento técnico u operativo, de las que se informará en el propio registro y en la sede electrónica.

2. Al efecto del cómputo de los plazos, la sede electrónica mostrará en lugar fácilmente visible la fecha y hora oficial de la sede, que será la que conste como fecha y hora de la transacción, adoptando las medidas precisas para asegurar su integridad. Las personas interesadas podrán manifestar su discrepancia respecto a dichas fecha y hora en el acto mismo de presentación de los correspondientes formularios.

3. El cómputo de plazos se realizará conforme a lo dispuesto en los apartados 3, 4 y 5 del artículo 26 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos. A estos efectos el Registro se regirá por la fecha y la hora oficial española, correspondiente a la península, Ceuta, Melilla y el archipiélago balear.

4. El Registro Electrónico especificará el calendario de días inhábiles relativo a sus procedimientos y trámites, que será el que se determine en la resolución anual publicada en el «Boletín Oficial del Estado» para todo el territorio nacional por el Ministerio de la Presidencia.

5. Cuando la ineludible realización de trabajos de mantenimiento u otras razones técnicas lo requieran, podrán planificarse paradas de los sistemas informáticos que afecten o imposibiliten de forma temporal el servicio de comunicaciones telemáticas. Estas paradas serán avisadas por el propio sistema con la antelación que, en caso, resulte posible. En supuestos de interrupción no planificada en el funcionamiento del Registro Telemático, y siempre que sea posible, se comunicará dicha circunstancia.

Artículo 6. *Resguardo acreditativo de la presentación.*

El Registro Electrónico emitirá automáticamente un resguardo acreditativo de la presentación del escrito, solicitud o comunicación de que se trate, en el que constarán los datos proporcionados por la persona interesada con indicación de la fecha y hora en que tal presentación se produjo en el servidor de aquél. Dicho resguardo se configurará de forma que pueda ser impreso y su contenido se ajustara a lo establecido en el artículo 30.3 del Real Decreto 1671/2009, de 6 de noviembre.

Artículo 7. *Gestión, disponibilidad y Seguridad del Registro.*

La Secretaría General de la Agencia Española de Protección de Datos será el órgano responsable de la administración, gestión, disponibilidad y seguridad del Registro Electrónico del Agencia Española de Protección de Datos creado y regulado por la presente Resolución.

En la página de Internet de la Agencia Española de Protección de Datos, o en su sede electrónica estará disponible para consulta un resumen de los protocolos de seguridad del Registro.

El Registro Electrónico dispondrá los medios organizativos y técnicos adecuados para garantizar la interoperabilidad y seguridad de acuerdo con lo previsto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad y en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad y la normativa sobre protección de datos de carácter personal según lo previsto en el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

El Registro Electrónico observará los requisitos de accesibilidad previstos en el Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el reglamento sobre condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social. En este sentido las páginas web relacionadas con el Registro Electrónico deberán ajustarse a la prioridad 1 de la Norma UNE 139803:2004.

Artículo 8. *Requisitos de la documentación complementaría.*

Los formatos de los documentos electrónicos y de las imágenes electrónicas de los documentos serán establecidos en el marco del Esquema Nacional de Interoperabilidad. De acuerdo con los Instrumentos informáticos y vías de comunicación disponibles, podrá limitarse la extensión máxima de los documentos complementarios a presentar en una sola sesión.

La presentación de solicitudes, escritos y comunicaciones podrá incorporar como documentación complementaría:

a) Los documentos que cumplan los requisitos técnicos que se regulan en e la presente Resolución.

b) Los documentos no disponibles en formato electrónico y que, por su naturaleza, no sean susceptibles de aportación utilizando el procedimiento de copia digitalizada previsto en el artículo 35.2 de la Ley 11/2007, de 22 de junio, podrán incorporarse a través de las vías previstas en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, en el plazo de 10 días desde la presentación del correspondiente formulario electrónico. El incumplimiento de este plazo para aportación de la documentación complementaria, podrá dar lugar a su requerimiento conforma a lo dispuesto en el artículo 71 de la Ley 30/1992, de 26 de noviembre.

c) Siempre que se realice la presentación de documentos electrónicos separadamente el formulario principal, el interesado deberá mencionar el número o código de registro individualizado que permita identificar el expediente en el que haya de surtir efectos.

d) Los usuarios admiten con carácter exclusivo la responsabilidad de la custodia de los elementos necesarios para su autenticación en el acceso a estos servicios, el establecimiento de la conexión precisa y la utilización de la firma electrónica, así como de las consecuencias que pudieran derivarse del uso indebido, incorrecto o negligente de los mismos. Igualmente será responsabilidad del usuario la adecuada custodia y manejo de los ficheros que sean devueltos por el registro Electrónico como acuse de recibo.

Artículo 9. *Tratamiento de datos de carácter personal.*

Las anotaciones registrales de los asientos electrónicos efectuados en el Registro Electrónico se incorporarán al «Fichero de Entrada y Salida de Documentos» modificado en la Resolución de 24 de marzo de 2009, de la Agencia Española de Protección de Datos, por la que se crean, modifican y suprimen ficheros de datos de carácter personal de la Agencia, publicada en el BOE de 7 de abril de 2009.

Artículo 10. *Publicación de nuevos procedimientos de la Agencia Española de Protección de Datos.*

La admisión de nuevos procedimientos, trámites, preimpresos, solicitudes y modelos que en su caso sea acordada por Resolución de la Agencia Española de Protección de Datos será difundida a través de la página de Internet de la Agencia y en su sede electrónica.

Disposición transitoria.

Durante el plazo de seis meses contados desde la entrada en vigor de esta Resolución seguirá existiendo, de manera subordinada al Registro Electrónico de la Agencia Española de Protección de Datos, el Registro Telemático creado por Resolución de 12 de julio de 2006 de la Agencia Española de Protección de Datos, asociado a la aplicación de Notificación Telemática de la Agencia Española de Protección de Datos (NOTA).

Disposición derogatoria única.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Resolución.

Disposición final única. *Entrada en vigor.*

La presente Resolución entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO I

Procedimientos competencia de la Agencia Española de Protección de Datos admisibles a través de su Registro Electrónico

Registro General de Protección de Datos

1. Notificación de la creación, modificación o supresión de ficheros con datos de carácter personal para su inscripción en el Registro General de Protección de Datos.

Se puede realizar mediante el formulario electrónico de Notificaciones Telemáticas a la AEPD (NOTA) con certificado de firma electrónica reconocido. También se podrán enviar notificaciones de ficheros a la AEPD mediante formato XML igualmente firmadas con certificado de firma electrónica reconocido.

Las especificaciones técnicas para la remisión de notificaciones en este formato se encontrarán disponibles en la página web de la AEPD (www.agpd.es y en sedeagpd.gob.es).

Esta presentación tendrá carácter voluntario para los interesados, siendo alternativa la utilización de los Registros u oficinas a los que se refiere el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

§ 11

Resolución de 18 de marzo de 2010, de la Agencia Española de Protección de Datos, por la que se crea la Sede Electrónica de la Agencia Española de Protección de Datos

Agencia Española de Protección de Datos
«BOE» núm. 72, de 24 de marzo de 2010
Última modificación: sin modificaciones
Referencia: BOE-A-2010-4854

La incorporación de las tecnologías de la información y de las comunicaciones a la organización y funcionamiento de las Administraciones Públicas constituye un elemento clave para la garantía de la igualdad, la eficacia y la eficiencia en el acceso de los ciudadanos a los servicios públicos.

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, ya instó a las Administraciones Públicas a impulsar el empleo de los medios electrónicos en el ejercicio de sus competencias.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, ha supuesto un salto cualitativo en la implantación de las tecnologías de la información y del conocimiento en el seno de las Administraciones Públicas al reconocer el derecho de los ciudadanos a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/1992, de 26 de noviembre. El respeto y la salvaguarda del ejercicio de este derecho implica el reconocimiento de la obligación de las Administraciones Públicas de dotarse de los medios y sistemas electrónicos adecuados.

En particular, el artículo 10 de la Ley 11/2007, de 22 de junio, regula la creación de la sede electrónica como aquella dirección electrónica disponible para los ciudadanos a través de las redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.

De conformidad con el artículo 3.2 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, la sede electrónica se crea mediante orden del Ministro correspondiente o resolución del titular del organismo público, en la que deberán expresarse, como mínimo, los extremos citados por dicho precepto.

A su vez, conforme a la disposición final cuarta del Real Decreto 1671/2009, «los puntos de acceso electrónico pertenecientes a la Administración General del Estado o sus organismos públicos dependientes o vinculados en los que se desarrollan actualmente comunicaciones con terceros, propias de sede electrónica, deberán adaptarse, en el plazo de cuatro meses, contados a partir de la entrada en vigor de este Real Decreto, a lo dispuesto en el mismo para las sedes o, en su caso, subsedes, electrónicas, sin perjuicio de

lo previsto en las disposiciones transitorias primera y segunda de este Real Decreto y en la disposición final tercera de la Ley 11/2007, de 22 de junio».

En su virtud, previo informe de la Abogacía del Estado en la Agencia Española de Protección de Datos, resuelvo:

Artículo 1. *Objeto.*

La presente resolución tiene por objeto la creación de la sede electrónica de la Agencia Española de Protección de Datos (en adelante, AEPD), así como la regulación de su funcionamiento.

Artículo 2. *Creación de la sede electrónica de la AEPD y ámbito de la misma.*

1. En aplicación del artículo 10 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y del artículo 3 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, se crea la sede Electrónica de la AEPD.

Dicha sede será común a todos los órganos que integran la estructura de esta Agencia.

Artículo 3. *Dirección electrónica y acceso a la sede.*

La dirección electrónica de referencia de la sede electrónica de la AEPD es https://sedeagpd.gob.es, que será accesible directamente así como a través del portal de Internet http://www.agpd.es.

Artículo 4. *Titular y órganos encargados de la gestión y de los servicios.*

1. La titularidad de la sede electrónica de la AEPD corresponde a la AEPD.

2. El órgano encargado tanto de la gestión de la sede electrónica como de los servicios disponibles para los ciudadanos en esta sede es la Secretaría General de la AEPD.

Artículo 5. *Canales de acceso a los servicios disponibles en la sede electrónica de la AEPD.*

Los canales de acceso a los servicios disponibles en la sede electrónica de la AEPD serán:

a) Acceso electrónico, a través de Internet, según los principios de accesibilidad y usabilidad establecidos en la Ley 11/2007, de 22 de junio, en los términos dictados por la normativa vigente en cada momento, en su sede electrónica.

b) Atención presencial en las oficinas de la AEPD, sin perjuicio del acceso a través de los registros regulados en el artículo 38 de la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

c) Atención telefónica, a través del servicio que se hará constar en la propia sede electrónica y el portal de la Agencia. Al tiempo de entrada en vigor de esta Resolución, el servicio se sustenta en los teléfonos 901 100 099 y 91 266 35 17

Artículo 6. *Medios para la formulación de quejas y sugerencias.*

1. Los medios disponibles para la formulación de quejas y sugerencias en relación con el contenido, gestión y servicios ofrecidos en la sede electrónica de la AEPD serán:

a) Presencial o por correo postal en la dirección de la Agencia Española de Protección de Datos, calle Jorge Juan, 6, 28001 Madrid ,o de cualquier otro órgano administrativo, de conformidad con lo dispuesto en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre.

b) Presentación telemática a través de la sede electrónica de la AEPD

2. No se considerarán medios para la formulación de quejas y sugerencias los servicios de información y asesoramiento al ciudadano en la utilización de la sede electrónica.

Artículo 7. *Contenidos de la sede.*

1. La sede electrónica de la AEPD dispondrá del contenido y de los servicios a disposición de los ciudadanos previstos expresamente en el artículo 6 del Real Decreto 1671/2009, de 6 de noviembre.

2. Los contenidos publicados en la sede electrónica de la AEPD responderán a los criterios de seguridad e interoperabilidad que derivan de la Ley 11/2007, de 22 de junio, y de los Reales Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

Disposición final. *Entrada en vigor.*

La presente resolución entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 12

Resolución de 1 de septiembre de 2006, de la Agencia Española de Protección de Datos, por la que se determina la información que contiene el Catálogo de ficheros inscritos en el Registro General de Protección de Datos

Agencia Española de Protección de Datos
«BOE» núm. 227, de 22 de septiembre de 2006
Última modificación: 13 de noviembre de 2008
Referencia: BOE-A-2006-16580

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), publicada en el «Boletín Oficial del Estado» de 14 de diciembre, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

El artículo 39 de la LOPD regula el Registro General de Protección de Datos, como órgano integrado en la Agencia Española de Protección de Datos al que corresponde velar por la publicidad de los tratamientos y ficheros de datos personales existentes con la finalidad de facilitar al ciudadano el ejercicio de los derechos de acceso, rectificación, cancelación y oposición que la propia Ley le reconoce.

El derecho de consulta al Registro, regulado en el artículo 14 de la LOPD habilita a cualquier persona para conocer, de forma pública y gratuita, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del fichero.

Hasta ahora, en aplicación del citado artículo 14 de la LOPD, se han venido publicando los datos correspondientes a la identidad del responsable, la dirección ante la que pueden ejercerse los derechos de acceso, rectificación, cancelación y oposición, el nombre y la finalidad del fichero, y, en el caso de los ficheros de titularidad pública, los datos relativos a la disposición general de creación de cada uno de los ficheros inscritos en el Registro General de Protección de Datos.

Entre las funciones de la Agencia Española de Protección de Datos, de acuerdo a lo establecido en el artículo 37.1.j) de la Ley Orgánica 15/1999, se encuentra la de velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto debe publicar periódicamente una relación de dichos ficheros con la información adicional que determine el Director de la Agencia.

En consonancia con lo anterior, el artículo 7 del Real Decreto 428/1993, de 26 de marzo, establece que la Agencia Española de Protección de Datos, a efectos de dar publicidad de la existencia de ficheros con datos de carácter personal, publicará y difundirá un catálogo anual de los ficheros inscritos en el Registro General de Protección de Datos, con expresión de la información que al amparo del citado artículo 37.1.j) de la LOPD, determine el Director.

En la página web de la Agencia Española de Protección de Datos (www.agpd.es) se encuentra disponible el catálogo de ficheros inscritos en el Registro General de Protección

de Datos con el objeto de difundir y dar publicidad a la existencia de ficheros de datos de carácter personal, haciendo públicos hasta este momento los datos correspondientes a la identidad del responsable, la dirección de acceso, el nombre, la descripción y la finalidad del fichero.

Tras la aprobación de los nuevos formularios electrónicos (Sistema NOTA) por los que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos, por Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, publicada en el «Boletín Oficial del Estado» número 181, de 31 de julio de 2006, se han acometido modificaciones en la infraestructura tecnológica de la Agencia que hacen posible mejorar las condiciones de la publicación de los ficheros inscritos en el Registro General de Protección de Datos regulada en el artículo 37.1.j, con el objeto de facilitar el derecho de consulta regulado en el artículo 14 de la Ley, y ampliar la información que se facilita en el catálogo de ficheros.

En su virtud, y de conformidad con lo dispuesto en el citado artículo 37.1. j) de la Ley Orgánica 15/1999, de 13 de diciembre, resuelvo:

Primero.

Aprobar la información que contiene el catálogo de ficheros con datos de carácter personal inscritos en el Registro General de Protección de Datos que se incorporará a la edición que anualmente realiza la Agencia Española de Protección de Datos en CD-ROM o en el soporte que en función de la evolución de la tecnología se determine, y cuya finalidad es facilitar al ciudadano el ejercicio de los derechos de acceso, rectificación, cancelación y oposición regulados en los artículos 14 a 16 de la LOPD.

Segundo.

Aprobar la publicación del nuevo catálogo de los ficheros con datos de carácter personal inscritos en el Registro General de Protección de Datos, que estará disponible en forma gratuita en la página web de la Agencia Española de Protección de Datos (www.agpd.es), con actualización diaria, y cuya finalidad es facilitar al ciudadano el ejercicio de los derechos de acceso, rectificación, cancelación y oposición regulados en los artículos 14 a 16 de la LOPD.

Tercero.

La información que se hace pública en los catálogos que se aprueban en los apartados primero y segundo de esta Resolución se corresponde con la información que el responsable del fichero ha notificado al Registro General de Protección de Datos en los apartados siguientes: Responsable del fichero, servicio o unidad ante el que pueden ejercitarse los derechos de oposición, acceso, rectificación y cancelación, identificación y finalidad y usos previstos del fichero, origen y procedencia de los datos, incluyendo el colectivo de personas sobre el que se obtienen los datos de carácter personal, tipos de datos, estructura y organización del fichero y, en su caso, los destinatarios de cesiones y/o transferencias internacionales de datos. Además, en el caso de los ficheros de titularidad pública, se publicarán los datos relativos a la disposición general de creación, modificación o supresión del fichero.

En el caso de responsables de ficheros que actúen como persona física, no se publicará el dato relativo a su NIF.

Cuarto.

Los datos de carácter personal incluidos en los catálogos citados en los puntos primero y segundo, no podrán ser objeto de tratamiento, ni usarse para finalidades a las previstas en el artículo 14 de la LOPD.

Queda prohibida la reproducción total o parcial de los catálogos a que se refiere la presente Resolución, incluso el volcado del contenido en cualquier soporte, sin expresa autorización de la Agencia Española de Protección de Datos.

Quinto.

En ningún caso podrá tomarse la presencia o ausencia de un fichero en estos catálogos como certificación positiva o negativa de una inscripción en el Registro General de Protección de Datos.

Sexto.

La presente Resolución entrará en vigor al día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 13

Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se crea el Registro Telemático de la Agencia Española de Protección de Datos

Agencia Española de Protección de Datos
«BOE» núm. 181, de 31 de julio de 2006
Última modificación: sin modificaciones
Referencia: BOE-A-2006-13848

La Agencia Española de Protección de Datos es un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones, y que tiene por objeto la garantía del cumplimiento y aplicación de las previsiones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y sus normas de desarrollo.

El art. 35.2 de la LOPD establece que en el ejercicio de sus funciones públicas, y en defecto de lo que disponga la propia LOPD y sus disposiciones de desarrollo, la Agencia Española de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

El art. 45 de la Ley 30/1992 prevé que las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias. En igual sentido, la reforma de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común efectuada por la Ley 24/2001, de 27 de diciembre, de medidas Fiscales, Administrativas y del Orden Social, tuvo por finalidad potenciar el uso de medios electrónicos, informáticos y telemáticos por la Administración.

Las previsiones de la Ley 30/1992, de 26 de diciembre fueron desarrolladas por el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, y que fue modificado por el Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

El Real Decreto 209/2003 modificó igualmente el Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro, añadiendo un nuevo capítulo dedicado a la regulación de los Registros Telemáticos.

Por su parte, el artículo 4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, establece que esta ley es de aplicación al uso de la firma en el seno de las administraciones

Públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquellas y éstos entre sí o con los particulares.

Teniendo en cuenta los preceptos legales citados anteriormente, la presentación por vía telemática de solicitudes, escritos y comunicaciones requiere la creación de un registro telemático que se ocupe de la recepción y remisión de los mismos, y la especificación de los procedimientos en que dicho registro podrá ser utilizado, de acuerdo con el artículo 38, apartado 9, de la Ley 30/1992, de 26 de noviembre.

En su virtud, y de conformidad con lo dispuesto en el artículo 37.1.c) de la Ley Orgánica 5/1999, de 13 de diciembre, resuelvo:

Primero. *Objeto.*

La presente resolución tiene por objeto la creación y regulación del Registro Telemático de la Agencia Española de Protección de Datos, encargado de la recepción de y remisión de solicitudes, escritos, y comunicaciones, así como el establecimiento de los requisitos y condiciones de funcionamiento de dicho registro respecto de los trámites y procedimientos comprendidos dentro de su ámbito de aplicación.

Segundo. *Ámbito de aplicación.*

El Registro Telemático de la Agencia Española de Protección de Datos estará habilitado para los procedimientos de notificación de ficheros con datos de carácter personal para su inscripción en el Registro General de Protección de Datos mediante el formulario electrónico de Notificaciones Telemáticas a la AEPD (NOTA) con certificado de firma electrónica reconocido. También se podrán enviar notificaciones de ficheros a la AEPD mediante formato XML igualmente firmadas con certificado de firma electrónica reconocido. Las especificaciones técnicas para la remisión de notificaciones en este formato se encontrarán disponibles en la página web de la AEPD (www.agpd.es).

Esta presentación tendrá carácter voluntario para los interesados, siendo alternativa la utilización de los Registros u oficinas a los que se refiere el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

La recepción en el Registro Telemático de la Agencia Española de Protección de Datos de solicitudes, escritos y comunicaciones que no estén incluidas en lo especificado en el ámbito de aplicación, o que hayan sido presentadas por medios diferentes al telemático no producirá ningún efecto. En estos casos, se archivarán, teniéndolas por no presentadas y comunicándolo así al remitente.

El Director de la Agencia Española de Protección de Datos podrá ordenar, mediante la oportuna resolución, la inclusión de nuevos procedimientos y trámites, para los que será válido lo dispuesto en esta Resolución, así como aprobar los modelos normalizados de obligatoria utilización para su recepción y remisión a través del Registro Telemático.

La relación actualizada de solicitudes, escritos y comunicaciones relativos a los trámites y procedimientos que puedan presentarse en el Registro Telemático de la Agencia Española de Protección de Datos figurará en la dirección electrónica de acceso al registro (www.agpd.es).

Tercero. *Creación del Registro Telemático de la Agencia Española de Protección de Datos.*

1. Se crea el Registro Telemático de la Agencia Española de Protección de Datos para la recepción y remisión de solicitudes, escritos y comunicaciones relativas a los trámites y procedimientos que se especifican en el apartado segundo de esta Resolución, que se remitan y expidan mediante firma electrónica en aplicación de lo previsto en el artículo 38.9 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. En defecto de lo que pueda disponer la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y sus disposiciones de desarrollo, resultará de aplicación lo dispuesto en el Real Decreto 263/1996, de 16 de febrero, de utilización de técnicas electrónicas, Informáticas y telemáticas por la Administración General del Estado, así como en el Real Decreto 772/1999, de 7 de mayo, que regula la presentación de

solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devoluciones de originales y el régimen de las oficinas de registro, y la Orden PRE/1551/2003, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, que regula los registros y notificaciones telemáticas, así como la utilización de los medios telemáticos para la sustitución de certificados por los ciudadanos.

3. El Registro Telemático de la Agencia Española de Protección de Datos, se configura como un registro auxiliar del Registro de Entrada y Salida de este Ente Público, en los términos previstos en el apartado 4 del artículo 7 del Real Decreto 263/1996.

4. El acceso al Registro Telemático de la Agencia Española de Protección de Datos por los interesados se realizará a través de la dirección electrónica de la Agencia (www.agpd.es).

Cuarto. *Requerimientos técnicos necesarios para el acceso al Registro Telemático de la Agencia Española de Protección de Datos.*

1. El acceso de los ciudadanos interesados en comunicarse con el Registro Telemático se realizará a través de Internet mediante el correspondiente navegador web. En la dirección electrónica de acceso al Registro Telemático estará disponible la relación de los sistemas operativos y navegadores que puedan ser utilizados por los interesados.

2. Cuando así lo prevea la norma de aprobación de los modelos utilizados para el envío y recepción de solicitudes, escritos y comunicaciones telemáticas relacionadas con los trámites y procedimientos incluidos en el ámbito del Registro Telemático, se permitirá el acceso a través de tecnologías que permitan la comunicación directa entre éste y las aplicaciones desarrolladas por los interesados o por la propia Agencia. En estos casos, la norma de aprobación de los modelos y comunicaciones telemáticas deberá especificar los formatos de intercambio de datos, y las especificaciones técnicas necesarias para el envío y recepción de los documentos.

3. De acuerdo con el principio de neutralidad tecnológica, los requisitos técnicos necesarios para el acceso al Registro Telemático de la Agencia se adecuarán en lo posible a los estándares y directrices que favorezcan su interoperabilidad y su compatibilidad con el mayor número de herramientas informáticas posible, como navegadores y sistemas operativos.

Quinto. *Sistemas de firma electrónica reconocidos.*

1. Las solicitudes, escritos y comunicaciones recibidas o remitidas por el Registro Telemático estarán firmados electrónicamente, utilizando sistemas de firma electrónica según lo previsto en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, y teniendo en cuenta las normas adicionales recogidas en el artículo 4 de la mencionada Ley. Los certificados deberán ser conformes con la recomendación UIT X.509.

2. En la dirección electrónica de acceso al Registro Telemático estará disponible la información sobre la relación de prestadores de servicios de certificación y tipos de certificados electrónicos que amparen las firmas electrónicas utilizadas en la recepción y remisión de solicitudes, escritos y comunicaciones.

Sexto. *Recepción de solicitudes y cómputo de plazos.*

1. La presentación de solicitudes, escritos y comunicaciones al Registro Telemático podrá realizarse durante las 24 horas de todos los días del año. El Registro Telemático se regirá por la fecha y hora oficial española correspondiente a la península y al archipiélago Balear, que deberá figurar visible en la dirección electrónica de acceso al Registro.

2. El Registro Telemático emitirá por el mismo medio, y utilizando los sistemas que se determinen en función del procedimiento o trámite, un mensaje de confirmación de la solicitud, escrito o comunicación en el que constarán los datos proporcionados por el interesado, junto con la acreditación de la fecha y hora en que produjo la recepción y una clave de identificación de la transmisión. El mensaje de confirmación se configurará de forma que pueda ser impreso o archivado informáticamente por el interesado y que garantizará la

identidad del registro, tendrá el valor de recibo de presentación a efectos de lo dispuesto en el artículo 6.3 del Real Decreto 772/1999.

3. El usuario deberá ser advertido de que la no recepción del mensaje de confirmación, o en su caso, la recepción de un mensaje de indicación de error implica que no se ha producido la recepción del mismo, debiendo realizarse la presentación en otro momento o utilizando otros medios.

4. A los efectos del cómputo de plazo, la recepción en un día inhábil se entenderá efectuada el primer día hábil siguiente. En este caso, en el asiento de entrada se inscribirán como fecha y hora de presentación aquéllas en que se produjo efectivamente la recepción, constando como fecha y hora de entrada las cero horas y un segundo del primer día hábil siguiente.

5. El calendario de días inhábiles a efectos de este Registro Telemático será el que se determine en la resolución anual publicada en el Boletín Oficial del Estado para todo el territorio nacional por el Ministerio de Administraciones Públicas, según lo dispuesto en el artículo 48.7 de la Ley 30/1992.

6. El Registro Telemático de la Agencia Española de Protección de Datos no realizará ni anotará salidas de escritos y comunicaciones en días inhábiles.

7. Cuando la ineludible realización de trabajos de mantenimiento u otras razones técnicas lo requieran, podrán planificarse paradas de los sistemas informáticos que afecten o imposibiliten de forma temporal el servicio de comunicaciones telemáticas. Estas paradas serán avisadas por el propio sistema con la antelación que, en su caso, resulte posible. En supuestos de interrupción no planificada en el funcionamiento del Registro Telemático, y siempre que sea posible, se comunicará dicha circunstancia.

Séptimo. *Seguridad.*

1. La Secretaría General de la Agencia Española de Protección de Datos será la responsable de la seguridad del Registro Telemático de la Agencia Española de Protección de Datos.

2. En la dirección electrónica del Registro Telemático estará disponible información actualizada sobre los protocolos de seguridad del registro y de las transacciones telemáticas.

Octavo. *Accesibilidad.*

1. La Agencia Española de Protección de datos tomará las medidas necesarias para lograr un adecuado nivel de accesibilidad con el fin de que el Registro Telemático pueda ser utilizado por personas discapacitadas o de edad avanzada.

2. Las páginas web de la Agencia Española de Protección de Datos relacionadas con el Registro Telemático se adecuaran a las Directrices de Accesibilidad WAI 1.0 del W3C al menos en su nivel AA.

3. Los formularios electrónicos aprobados para su remisión al Registro Telemático o los programas que a tal efecto pudiera desarrollar la Agencia Española de Protección de Datos incorporarán un grado de accesibilidad similar en función del estado de la tecnología utilizada en cada caso.

Noveno. *Entrada en vigor.*

La presente resolución entrará en vigor el día 1 de septiembre de 2006.

§ 14

Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos, así como los formatos y requerimientos a los que deben ajustarse las notificaciones remitidas en soporte informático o telemático

Agencia Española de Protección de Datos
«BOE» núm. 181, de 31 de julio de 2006
Última modificación: sin modificaciones
Referencia: BOE-A-2006-13849

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), publicada en el Boletín Oficial del Estado de 14 de diciembre, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

En su artículo 39, la LOPD prevé la existencia de un Registro General de Protección de Datos (RGPD), como órgano integrado en la Agencia Española de Protección de Datos al que corresponde velar por la publicidad de los tratamientos y ficheros de datos personales existentes con la finalidad de facilitar al ciudadano el ejercicio de los derechos que la propia Ley le reconoce.

A este fin establece la obligación de notificar los ficheros de carácter personal para su inscripción en el RGPD, a aquellas personas físicas o jurídicas, de naturaleza pública o privada, u órganos administrativos, que procedan a la creación de ficheros con datos de carácter personal, con carácter previo a la misma.

Esta obligación de notificar los ficheros implica la puesta en práctica de unos procedimientos de inscripción para poder tramitar un número creciente de notificaciones.

La notificación de ficheros al Registro está regulada en los artículos 20 y 26 de la LOPD, estableciéndose el procedimiento a través del cual se realiza la misma en el Real Decreto 1332/1994, de 20 de junio, que desarrolla determinados aspectos de la derogada Ley Orgánica 5/1992, cuyos artículos 5 y 6 habilitan a la Agencia Española de Protección de Datos para elaborar modelos normalizados de solicitud de inscripción para los ficheros de titularidad pública o privada, respectivamente. El Real Decreto 1332/1994 continúa vigente, según declara expresamente la Disposición transitoria tercera de la Ley Orgánica 15/1999, en cuanto no se oponga a la misma.

Mediante Resolución de 30 de mayo de 2000, de la Agencia Española de Protección de Datos, publicada en el Boletín Oficial del Estado n.º 153, de 27 de junio de 2000, se aprobaron los modelos normalizados en soporte papel, magnético y telemático a través de

los que debe efectuarse la notificación de los ficheros y su solicitud de inscripción en el Registro General de Protección de Datos. Estos modelos reemplazaron a los establecidos en la Resolución de la Agencia Española de Protección de Datos de 22 de junio de 1994, publicada en el Boletín Oficial del Estado de 23 de junio de 1994, a fin de proceder a su adaptación a los nuevos requerimientos previstos en la LOPD.

El artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, insta a las Administraciones Públicas a promover la incorporación de técnicas electrónicas, informáticas y telemáticas en el desarrollo de su actividad y el ejercicio de sus competencias. En este sentido, y como consecuencia del compromiso de la Agencia Española de Protección de Datos con la administración electrónica, la resolución de 30 de mayo de 2000, incluía la aprobación de los modelos de notificación de ficheros en soporte magnético y telemático, así como la del programa informático de generación de notificaciones, permitiendo de ese modo la remisión de las solicitudes de inscripción en soporte informático o a través de Internet, con el requisito de la presentación convencional de la correspondiente hoja de solicitud debidamente cumplimentada y firmada.

La implantación de la administración electrónica exige que se realicen, entre otras, acciones encaminadas a la simplificación administrativa y a la adaptación normativa tendente a permitir una eficaz aplicación de las soluciones tecnológicas. A su vez, el desarrollo de la sociedad de la información y la difusión de los efectos positivos que de ella se derivan exige la generalización de la confianza de la ciudadanía en las comunicaciones telemáticas.

En este sentido, debía abordarse la incorporación de procedimientos que permitiesen la utilización de la firma electrónica en el proceso de notificación de tratamientos a través de Internet, eliminando los trámites añadidos que debían verificarse en formato papel y agilizando y facilitando el procedimiento de notificación.

La Ley 59/2003, de 19 de diciembre, de firma electrónica, regula en su artículo 4, el empleo de la firma electrónica en el ámbito de las Administraciones Públicas. La incorporación de la firma electrónica al procedimiento de notificación electrónica de inscripción de ficheros, elimina la necesidad de la presentación convencional de la hoja de solicitud.

Además, en el Real Decreto 1553/2005, de 23 de diciembre, que regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, se establece que la firma electrónica realizada a través del documento nacional de identidad tendrá respecto a los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Por otra parte, la Agencia debe llevar a la práctica las recomendaciones incluidas en el informe sobre la simplificación de los requerimientos para la notificación que, como consecuencia del primer informe sobre implementación de la Directiva 95/46/CE, fue adoptado en el seno del Grupo de Trabajo de autoridades de protección de datos creado por el artículo 29 de esta Directiva.

En este informe se establece la conveniencia de profundizar en el régimen de excepciones de la notificación de determinados ficheros prevista en la Directiva 95/46. Si bien la LOPD establece el carácter obligatorio de la notificación de todos los ficheros, sí resulta posible establecer procedimientos que faciliten el cumplimiento de esta obligación en determinados supuestos.

Del actual sistema de información del RGPD se observa que el 35% de los ficheros de titularidad privada y el 20% de los de titularidad pública, lo que supone una tercera parte del total de ficheros declarados en el Registro, se corresponden con categorías concretas de ficheros.

Así sucede con los ficheros de clientes, recursos humanos, nóminas, comunidades de propietarios, pacientes, libro recetario de oficinas de farmacia, en relación con los ficheros de titularidad privada y con los de recursos humanos, gestión del padrón, gestión económica o control de acceso, en el caso de ficheros de titularidad pública.

Teniendo en cuenta lo anterior, se ha previsto poner a disposición de los responsables que realicen este tipo de tratamientos una serie de notificaciones ya cumplimentadas, a fin de facilitar la notificación de estos ficheros mediante el formulario electrónico.

En todo caso, las solicitudes de inscripción de ficheros deberán cumplimentarse mediante los formularios electrónicos aprobados en esta Resolución y que podrán ser presentados en soporte papel, informático o telemático. Dichos formularios estarán disponibles de forma gratuita en la página web de la AEPD (www.agpd.es).

Además se pone a disposición de los responsables un sistema de intercambio basado en mensajes en formato XML, con o sin certificado de firma electrónica, a través del que se podrán enviar notificaciones mediante la utilización de programas propios. Para ello se establecen las normas que deberán cumplir las aplicaciones desarrolladas por terceros para que puedan presentar validamente las notificaciones al RGPD.

Las hojas de solicitudes correspondientes a las notificaciones de ficheros enviadas por Internet podrán ser firmadas electrónicamente, debiendo presentarse en el Registro Telemático de la Agencia Española de Protección de Datos, de acuerdo con las normas y requisitos establecidos en la resolución por la que se crea dicho Registro Telemático.

Las notificaciones también podrán continuar enviándose por Internet sin firma electrónica, si bien, en ese caso, deberá cumplimentarse y firmarse la hoja de solicitud de inscripción generada por el formulario, que habrá de presentarse en la Agencia Española de Protección de Datos, o en cualquiera de los registros y oficinas a que se refiere el artículo 38.4 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Por último, mediante el formulario electrónico NOTA se podrán presentar notificaciones en formato papel, con la seguridad de que han sido correctamente cumplimentadas. Este formato de presentación incluye un código óptico de lectura para agilizar su inscripción en el RGPD.

Cuando las notificaciones hayan sido presentadas a través de Internet mediante certificado de firma electrónica reconocido, y así lo manifiesten los interesados expresamente en el formulario de notificación, podrán recibir por medios telemáticos la notificación de la resolución de inscripción, para lo que deberán disponer de una dirección electrónica a efectos de notificaciones del Servicio de Notificaciones Telemáticas Seguras.

Adicionalmente, los interesados que hayan presentado las notificaciones a través de Internet podrán consultar el estado de tramitación de su solicitud a través de la web de la AEPD.

Con los nuevos formularios electrónicos de Notificaciones Telemáticas a la AEPD (NOTA) se incorporan nuevos servicios electrónicos para facilitar el cumplimiento del trámite de notificación, al incorporar la posibilidad de su presentación telemática con firma electrónica, y que simplifican los modelos anteriores, mejorando los requisitos de accesibilidad y de independencia de plataforma informática.

Con el fin de que los responsables de ficheros puedan adaptarse a los nuevos formularios y teniendo en cuenta la amplia difusión y aceptación del programa de ayuda para la generación de notificaciones, se considera adecuado el establecimiento de un período transitorio durante el cual seguirán siendo válidos los modelos que preveía la Resolución de 30 de mayo de 2000, sin perjuicio de que sea también ya posible la presentación en los formularios que en la presente resolución se establecen. Este período concluirá, en cuanto a la presentación de notificaciones en soporte papel, el 1 de diciembre de 2006, a fin de garantizar el uso de medios electrónicos y telemáticos en el procedimiento.

Asimismo, a fin de garantizar la homogeneidad del Registro, se procederá a la adaptación de las inscripciones actualmente existentes y las que sean presentadas conforme a los modelos previstos en la Resolución de 30 de mayo de 2000 a los requerimientos derivados de esta Resolución.

Debe recordarse que la notificación de los ficheros en el Registro General de Protección de Datos tiene un carácter declarativo y la inscripción de un fichero en el RGPD, únicamente acredita que se ha cumplido con la obligación de notificación dispuesta en la Ley Orgánica 15/1999, sin que de esta inscripción se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones previstas en dicha Ley y demás disposiciones reglamentarias.

En su virtud, y de conformidad con lo dispuesto en el artículo 37.1.c de la Ley Orgánica 15/1999, de 13 de diciembre, resuelvo:

Primero.

Aprobar los formularios electrónicos NOTA a través de los que deberán efectuarse las solicitudes de inscripción en el Registro General de Protección de Datos. Dichos formularios estarán disponibles de forma gratuita en la página web de la Agencia Española de Protección de Datos (www.agpd.es), figurando su copia impresa en el anexo I de la presente Resolución.

Segundo.

Aprobar las normas de cumplimentación a las que habrán de adecuarse las notificaciones de ficheros de titularidad pública y privada en el Registro General de Protección de Datos y que figuran en el anexo II de esta Resolución.

Los formularios electrónicos de notificación de ficheros a la AEPD del sistema NOTA serán dinámicos y dispondrán de la correspondiente ayuda con el fin de facilitar su cumplimentación por el declarante.

En el caso de las inscripciones de alta de ficheros se mostrarán todos los apartados que definen el fichero, si bien únicamente deberán cumplimentarse los que correspondan en función del fichero objeto de la notificación.

En el caso de modificaciones, sólo se mostrarán aquellos apartados que el declarante haya señalado como objeto de la modificación.

En el caso de las supresiones, se mostrará el apartado correspondiente en el que deberá indicarse el motivo de la supresión y el destino que se dará a los datos o las previsiones que van a adoptarse para su destrucción.

Tanto para notificar una modificación como una supresión de la inscripción deberá hacerse constar en el formulario el código de inscripción asignado por la Agencia, así como los datos identificativos del responsable del fichero que figuran en la inscripción del mismo.

Tercero.

Las notificaciones, una vez cumplimentadas mediante el formulario electrónico de Notificaciones Telemáticas a la AEPD (NOTA), podrán remitirse a la Agencia Española de Protección de Datos en formato papel, soporte informático o a través de Internet, de acuerdo con las normas de cumplimentación a las que habrán de adecuarse las notificaciones de ficheros incluidas en el anexo II de esta Resolución.

Cuarto.

Mediante el formulario electrónico NOTA se podrán presentar notificaciones a través de Internet firmadas mediante certificado digital de firma reconocido de acuerdo con lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica. La relación actualizada de certificados de firma válidos para presentar notificaciones en el registro Telemático de la AEPD se podrá consultar en la página web de la AEPD.

Quinto.

Cuando la notificación se envíe a través de Internet sin certificado de firma electrónica reconocido, sólo se considerará recibida la notificación efectuada desde la fecha en la que tenga entrada en la Agencia Española de Protección de Datos la hoja de solicitud firmada de forma manual. En todo caso, carecerán de efecto alguno las notificaciones si la hoja de solicitud, debidamente cumplimentada y firmada, no hubiera sido presentada en la Agencia Española de Protección de Datos o en alguno de los Registros y oficinas a los que se refiere el artículo 38.4 de la Ley 30/1992, en el plazo de los diez días siguientes al envío de la notificación a través de Internet sin certificado de firma electrónica reconocido.

Sexto.

Podrán desarrollarse utilidades informáticas para la remisión de notificaciones al Registro General de Protección de Datos, debiendo las mismas atenerse al formato XML y a las

normas de cumplimentación aprobadas en el anexo II. Las especificaciones técnicas para la remisión de estos ficheros podrán consultarse en la página web de la AEPD.

Estos mensajes en formato XML pueden ser presentados con y sin certificado electrónico de firma reconocido. En el caso de que se presenten firmados electrónicamente deberán utilizar el estándar de firma Xml Digital Signature, cuya especificación de sintaxis y procesamiento se encuentra en http://www.w3.org/2000/09/xmldsig#. En este caso, una vez enviadas las notificaciones al Registro Telemático de la AEPD, éste devolverá un mensaje confirmando la recepción del envío incluyendo, a su vez, los datos necesarios para que el programa desarrollado por terceros configure el acuse de recibo de acuerdo con el formato que figura en el anexo III.

En el caso de que las notificaciones se presenten mediante formato XML sin certificado de firma electrónica, el servidor web de la AEPD devolverá un mensaje confirmando la recepción del envío e incluyendo, a su vez, los datos necesarios para que el programa desarrollado por terceros configure la Hoja de solicitud de acuerdo con el formato que figura en el anexo III. En todo caso, carecerán de efecto alguno las notificaciones si la hoja de solicitud, debidamente cumplimentada y firmada, no hubiera sido presentada en la Agencia Española de Protección de Datos o en alguno de los Registros y oficinas a los que se refiere el artículo 38.4 de la Ley 30/1992, en el plazo de los diez días siguientes al envío de las notificaciones a través de Internet mediante formato XML sin certificado de firma electrónica reconocido.

Séptimo.

Todas las recepciones de soportes informáticos y telemáticos serán provisionales, a resultas de su proceso y comprobación. Cuando no se ajusten al diseño y demás especificaciones establecidas en la presente Resolución, se requerirá al declarante para que subsane la notificación en el plazo de 10 días establecido en el artículo 71.1 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Si transcurrido dicho plazo no se hubiera recibido su notificación, se le tendrá por desistido de su petición, procediéndose sin más trámite al archivo de su solicitud.

Octavo.

Las versiones actualizadas de los formularios electrónicos de notificaciones Telemáticas a la AEPD, así como los anexos y requerimientos técnicos a los que se hace referencia en la presente Resolución estarán disponibles en la página web de la Agencia Española de Protección de Datos.

Noveno.

En tanto no se dicte una Resolución de la Agencia Española de Protección de Datos en que se señale expresamente lo contrario continuarán siendo válidas las notificaciones cumplimentadas con arreglo al programa de generación de notificaciones de ficheros de titularidad pública y privada aprobado mediante Resolución de la Agencia Española de Protección de Datos 30 de mayo de 2000.

Las notificaciones efectuadas mediante los formularios de notificación en soporte papel de ficheros de titularidad pública y privada, aprobados mediante Resolución de 30 de mayo de 2000, continuarán siendo válidas siempre que las mismas tengan entrada en la Agencia Española de Protección de Datos con anterioridad al 1 de diciembre de 2006.

Décimo.

El Registro General de Protección de Datos adecuará de oficio las notificaciones efectuadas conforme a los dos últimos párrafos del apartado anterior a los nuevos modelos aprobados mediante la presente Resolución.

Del mismo modo, procederá a la adecuación a los nuevos modelos de las notificaciones referidas a los ficheros inscritos en el Registro en la fecha de entrada en vigor de la presente Resolución.

Undécimo.

La presente Resolución entrará en vigor el día 1 de septiembre de 2006.

ANEXOS

Téngase en cuenta que se han omitido los Anexos que contienen los formularios que pueden consultarse en la página web de la Agencia Española de Protección de Datos www.agpd.es.

§ 15

Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras

Agencia Española de Protección de Datos
«BOE» núm. 296, de 12 de diciembre de 2006
Última modificación: sin modificaciones
Referencia: BOE-A-2006-21648

El incremento que últimamente están experimentando las instalaciones de sistemas de cámaras y videocámaras con fines de vigilancia ha generado numerosas dudas en lo relativo al tratamiento de las imágenes que ello implica. Además es un sector que ofrece múltiples medios de tratar datos personales como pueden ser los circuitos cerrados de televisión, grabación por dispositivos «webcam», digitalización de imágenes o instalación de cámaras en el lugar de trabajo. Precisamente la última Conferencia Internacional de Autoridades de Protección de Datos, celebrada en Londres los pasados días 1 a 3 de noviembre de este año, ha girado en torno a la necesidad de adecuar la videovigilancia a las exigencias del derecho fundamental a la protección de datos. Todo esto hace necesario que, en ejercicio de la competencia que le atribuye el artículo 37.1.c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la Agencia Española de Protección de Datos dicte una Instrucción para adecuar los tratamientos de imágenes con fines de vigilancia a los principios de dicha Ley Orgánica y garantizar los derechos de las personas cuyas imágenes son tratadas por medio de tales procedimientos.

El marco en que se mueve la presente Instrucción es claro. La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático.

Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999 y el artículo 1.4 del Real Decreto 1332/1994 de 20 de junio, que considera como dato de carácter personal la información gráfica o fotográfica.

En relación con la instalación de sistemas de videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por tanto, toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.

En consecuencia, el uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia por lo que, desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.

En cuanto a la proporcionalidad, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de «una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad.

En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)».

Asimismo la proporcionalidad es un elemento fundamental en todos los ámbitos en los que se instalen sistemas de videovigilancia, dado que son numerosos los supuestos en los que la vulneración del mencionado principio puede llegar a generar situaciones abusivas, tales como la instalación de sistemas de vigilancia en espacios comunes, o aseos del lugar de trabajo. Por todo ello se trata de evitar la vigilancia omnipresente, con el fin de impedir la vulnerabilidad de la persona.

Se excluyen de la presente Instrucción los datos personales grabados para uso o finalidad doméstica de conformidad con lo establecido en el artículo 2 a) de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, si bien en el sentido estricto señalado por el Tribunal de Justicia de las Comunidades Europeas en la Sentencia de 6 de noviembre de 2003, asunto Lindqvist, que al interpretar la excepción prevista en el artículo 3 apartado 2 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, indica que únicamente contempla «las actividades que se inscriben en el marco de la vida privada o familiar de los particulares» y no otras distintas. En la misma línea se pronuncia el Dictamen 4/2004, adoptado por el Grupo de Trabajo creado por el Artículo 29 de la Directiva 95/46/CE, con fecha 25 de noviembre de 2002.

Además, la Instrucción tampoco se aplicará al tratamiento de imágenes cuando éstas se utilizan para el ejercicio de sus funciones por parte de las Fuerzas y Cuerpos de Seguridad, que está cubierto por normas específicas, aunque estos tratamientos también deberán cumplir las garantías establecidas por la Ley Orgánica 15/1999.

Por otro lado, la Instrucción pretende adecuar los tratamientos a los criterios marcados por la jurisprudencia del Tribunal Constitucional al considerar que el tratamiento de datos personales no exige la conservación de los mismos, sino que basta su recogida o grabación. En el mismo sentido se han pronunciado las legislaciones que sobre esta materia han adoptado los distintos Estados miembros de la Unión Europea, cumpliendo así el mandato contenido en la Directiva 95/46/CE.

Por último, las plenas garantías de protección de los datos personales, así como las peculiaridades de su tratamiento exige una regulación concreta evitando la aplicación de un conjunto de reglas abstractas y dispersas. Por ello, a la hora de regular la legitimación del tratamiento de imágenes, la Agencia Española de Protección de Datos, entiende que es requisito esencial la aplicación íntegra del artículo 6.1 y 2 y del artículo 11.1 y 2 de la LOPD, sin perjuicio del estricto cumplimiento de los requisitos que para la instalación de cámaras o videocámaras de vigilancia vengan exigidos por la legislación vigente. Asimismo se regula el contenido del deber de información previsto en el artículo 5 de la misma Ley Orgánica, así como el ejercicio de los derechos a que se refieren los artículos 15 y siguientes de la citada Ley Orgánica. Por descontado, la creación de un fichero de videovigilancia exige su previa notificación a la Agencia Española de Protección de Datos, para la inscripción en su Registro General.

En su virtud, de conformidad con lo dispuesto en el artículo 37.1.c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, dispongo:

Artículo 1. *Ámbito objetivo.*

1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.

El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.

Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma.

2. El tratamiento de los datos personales procedentes de las imágenes obtenidas mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad se regirá por las disposiciones sobre la materia.

3. No se considera objeto de regulación de esta Instrucción el tratamiento de imágenes en el ámbito personal y doméstico, entendiéndose por tal el realizado por una persona física en el marco de una actividad exclusivamente privada o familiar.

Artículo 2. *Legitimación.*

1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia.

Artículo 3. *Información.*

Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:

a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y

b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción.

Artículo 4. *Principios de calidad, proporcionalidad y finalidad del tratamiento.*

1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

2. Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

Artículo 5. *Derechos de las personas.*

1. Para el ejercicio de los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, el/la afectado/a deberá remitir al responsable del tratamiento solicitud en la que hará constar su identidad junto con una imagen actualizada. El ejercicio de estos derechos se llevará a cabo de conformidad con lo dispuesto en la citada Ley Orgánica y su normativa de desarrollo.

2. El responsable podrá facilitar el derecho de acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento.

3. El/la interesado/a al que se deniegue total o parcialmente el ejercicio de los derechos señalados en el párrafo anterior, podrá reclamar su tutela ante el Director de la Agencia Española de Protección de Datos.

Artículo 6. *Cancelación.*

Los datos serán cancelados en el plazo máximo de un mes desde su captación.

Artículo 7. *Notificación de ficheros.*

1. La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.

Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.

Articulo 8. *Seguridad y Secreto.*

El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Asimismo cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas.

El responsable deberá informar a las personas con acceso a los datos del deber de secreto a que se refiere el apartado anterior.

Disposición transitoria.

Los responsables de ficheros de videovigilancia ya inscritos en el Registro General de la Agencia Española de Protección de Datos deberán adoptar las medidas previstas en el artículo 3, letra a), y en el artículo 4.3 de esta Instrucción en el plazo máximo de tres meses desde su entrada en vigor.

Disposición final.

La presente Instrucción entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

2. El modelo a que se refiere el apartado anterior, está disponible en la página web de la Agencia Española de Protección de Datos, www.agpd.es, de donde podrá ser descargado, especificando los datos del responsable.

§ 16

Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones

Agencia Española de Protección de Datos
«BOE» núm. 4, de 5 de enero de 2005
Última modificación: sin modificaciones
Referencia: BOE-A-2005-186

I

Uno de los objetivos fundamentales de la Agencia Española de Protección de Datos es el de lograr la mayor transparencia en su actividad, para una mejor garantía y tutela del derecho fundamental a la protección de datos de carácter personal, en el marco del proceso de implantación de la sociedad de la información.

Desde su creación, cada año se ha publicado una Memoria de la Agencia Española de Protección de Datos. A través de estas memorias se ha podido tener conocimiento de las actividades desarrolladas por la Agencia, de los procedimientos que se han seguido en la misma y de los criterios con que han sido resueltos. Sin embargo, dado el tiempo que transcurre desde que se dicta una resolución hasta que se publica la Memoria han podido existir desfases en el conocimiento del parecer de la Agencia.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, tras la modificación introducida por el artículo 82.1 de la Ley 62/2003, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, establece en el artículo 37.2 que las resoluciones de la Agencia Española de Protección de Datos, a excepción de las correspondientes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos y de aquéllas por las que se resuelva la inscripción en el mismo de los códigos tipo regulados en el artículo 32 de la citada Ley, se harán públicas, una vez hayan sido notificadas a los interesados, preferentemente a través de medios informáticos o telemáticos.

Con la modificación introducida por la citada Ley 62/2003, la Agencia tiene, por consiguiente, la obligación de hacer públicas sus resoluciones desde el momento en que han sido notificadas a los interesados, lo que sin duda redundará en un mejor conocimiento de sus criterios y una mayor seguridad jurídica en la aplicación de la Ley. Dado que dicha Ley entró en vigor el día 1 de enero de 2004, sus disposiciones en materia de publicidad de las resoluciones de la Agencia Española de Protección de Datos afectarán a todas aquéllas dictadas en procedimientos incoados a partir de dicha fecha, así como a las correspondientes al archivo de actuaciones inspectoras iniciadas desde esa misma fecha.

Con ello, se potencia el conocimiento de los criterios en la aplicación de la normativa sobre protección de datos, se facilita su cumplimiento y se favorece, asimismo, la aplicación de los principios de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de

octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

II

El artículo 37.1 c) de la Ley Orgánica 15/1999 atribuye a la Agencia Española de Protección de Datos la función de «dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley». La potestad normativa de la Agencia ha sido expresamente reconocida por el Tribunal Constitucional, en su Sentencia 290/2000, de 30 de noviembre.

En ejercicio de dicha potestad se dicta la presente Instrucción, cuyo objeto es establecer los términos en los que la Agencia Española de Protección de Datos va a realizar la publicación de las resoluciones a las que hace referencia el artículo 37.2 de la Ley Orgánica 15/1999.

Con dicho objeto, se establece la forma y los plazos en que se realizará la publicación de las indicadas resoluciones y, se prevé que, en todo caso, a fin de salvaguardar el derecho fundamental a la protección de datos de carácter personal, será necesario proceder a la disociación de dichos datos.

Asimismo, se dispone que en las resoluciones a las que se refiere el artículo 37.2 de la Ley Orgánica 15/1999, la Agencia hará constar, de forma expresa, que procederá a su publicación.

En su virtud, de conformidad con lo dispuesto en el artículo 37.1 c) de la Ley Orgánica 15/1999 y de acuerdo con el Consejo Consultivo de la Agencia Española de Protección de Datos,

DISPONGO:

Norma primera.

De conformidad con lo establecido en el artículo 37.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, según la redacción dada por el artículo 82.1 de la Ley 62/2003, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, la Agencia Española de Protección de Datos hará públicas sus resoluciones, a excepción de las correspondientes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos y de aquéllas por las que se resuelva la inscripción en el mismo de los códigos tipo regulados en el artículo 32 de la Ley Orgánica 15/1999, siempre que se refieran a procedimientos que se hubieran iniciado a partir del 1 de enero de 2004, o correspondan al archivo de actuaciones inspectoras incoadas desde dicha fecha.

Norma segunda.

La publicación de estas resoluciones se realizará en la página web de la Agencia Española de Protección de Datos, en el plazo de un mes a contar desde el día siguiente al de su notificación a los interesados.

Norma tercera.

En las resoluciones a las que se refiere la norma primera se hará constar expresamente que la Agencia va a proceder a su publicación en los términos establecidos en la presente Instrucción.

Norma cuarta.

La publicación de las resoluciones a que se refiere la presente Instrucción se realizará previa disociación de los datos de carácter personal a los que se refiere el artículo 3 a) de la Ley Orgánica 15/1999.

La publicación de dichas resoluciones no contendrá, en ningún caso, los datos referentes al domicilio de las personas jurídico privadas, empresarios individuales o profesionales afectados por la resolución.

Norma quinta.

Las resoluciones correspondientes a los procedimientos y actuaciones de inspección que se mencionan en la norma primera iniciados a partir del 1 de enero de 2004 y que hayan sido notificadas antes de la fecha de entrada en vigor de la presente Instrucción, se publicarán en el plazo de tres meses a partir de la misma.

Norma sexta.

La presente Instrucción entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

§ 17

Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos

Agencia de Protección de Datos
«BOE» núm. 301, de 16 de diciembre de 2000
Última modificación: sin modificaciones
Referencia: BOE-A-2000-22726

El régimen del movimiento internacional de datos de carácter personal ha sido, desde la aprobación de la derogada Ley Orgánica 5/1992, de 29 de octubre, de regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD), una de las cuestiones que ha suscitado un mayor número de dudas por parte de los responsables de los ficheros y la sociedad en general.

El motivo de estas dudas probablemente se encuentre en el hecho de que las normas reguladoras en esta materia contenidas en la Ley y sus normas de desarrollo hayan debido adaptarse a las incluidas en los artículos 25 y 26 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como por las Decisiones que, en cumplimiento de los citados preceptos se adopten por la Comisión de las Comunidades Europeas.

La actuación de la Agencia de Protección de Datos en sus casi siete años de existencia ha generado una abundante casuística relacionada con las transferencias internacionales de datos de carácter personal que hasta la fecha no venía recogida sistemáticamente en ningún texto.

Por otra parte, el artículo 37 c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, consagra la competencia de la Agencia de Protección de Datos para «dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley».

En uso de esta facultad, la presente Instrucción tiene por objeto señalar los criterios orientativos seguidos por la Agencia de Protección de Datos en relación con aquellos tratamientos que supongan una transferencia internacional de datos, poniendo de manifiesto el procedimiento que, en uso de las competencias que la Ley le atribuye, se sigue por la Agencia en cada caso concreto.

Por tanto no es finalidad de esta Instrucción efectuar innovación alguna dentro de la normativa reguladora de la protección de datos de carácter personal sino, simplemente, aclarar y facilitar a todos los interesados en un único texto, el procedimiento seguido por la Agencia para dar cumplimiento a las previsiones contenidas en la diversidad de normas que se refieren al movimiento internacional de datos.

II

Los artículos 33 y 34 de la Ley Orgánica 15/1999 establecen el régimen al que habrán de someterse los movimientos internacionales de datos. Estos preceptos, sin modificar el criterio general que habrá de regir las transferencias, esto es, la exigencia de autorización del Director de la Agencia de Protección de Datos, vienen a adecuar el régimen de excepciones a dicha autorización, añadiendo a los ya contemplados en la LORTAD otros deducidos de lo dispuesto en los artículos 25 y 26 de la Directiva 95/46/CE. En particular, el artículo 34 k) de la Ley Orgánica 15/1999 exceptúa del régimen general de autorización el supuesto en que «la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado».

En este sentido, deben tenerse en cuenta las recintes Decisiones de la Comisión de las Comunidades Europeas, números 2000/518/CE, 2000/519/CE y 2000/520/CE, de 26 de julio (publicadas en el Diario Oficial de las Comunidades Europeas de 25 de agosto de 2000), que consideraron adecuado el nivel de protección de datos personales en Suiza, Hungría, así como «el conferido por los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos».

El régimen regulador del movimiento internacional de datos se encuentra, en todo caso, gobernado por el principio general, contenido en el artículo 25.1 de la Directiva, de que la transferencia a empresas o Administraciones ubicadas en el territorio de terceros Estados deberá entenderse «sin perjuicio del cumplimiento de las disposiciones de derecho nacional adoptadas con arreglo a las disposiciones de la presente Directiva». En este mismo sentido se pronuncian las Decisiones de la Comisión de las Comunidades Europeas a las que acabamos de hacer referencia en su artículo 2.

III

A la vista de todo ello, la presente Instrucción se divide en dos Secciones:

La primera de ellas establece criterios predicables de la totalidad de las transferencias internacionales de datos, indicando los conceptos generales que han de ser tenidos en cuenta para el cumplimiento de lo indicado en la Ley. Se recuerda además en esta Sección el principio general referente al necesario cumplimiento de la Ley Orgánica 15/1999 por parte de aquellas personas o entidades que pretendan efectuar una transferencia internacional de datos. Por último, se señala el procedimiento que las normas vigentes prevén para la notificación de dicha transferencia a esta Agencia de Protección de Datos.

La segunda Sección se refiere a supuestos concretos de transferencias. En particular, se contemplan tres supuestos específicos, dos atendiendo al país al que los datos se destinen y uno en función de la finalidad última que motiva la transferencia.

Así, la norma cuarta se refiere a aquellos países no comunitarios respecto de los que se haya declarado la existencia de un nivel de protección adecuado, con especial referencia al supuesto contemplado por la Decisión 2000/520/CE, de la Comisión de las Comunidades Europeas, a la que ya se ha hecho referencia.

La norma quinta toma en consideración la solución contractual en el supuesto de transferencias que exijan la autorización del Director de la Agencia de Protección de Datos, conforme a lo dispuesto en el artículo 33 de la Ley Orgánica 15/1999, indicando aquellos extremos que la Agencia ha venido considerando necesarios para que se entienda que la transferencia ofrece un adecuado nivel de garantía. La solución contractual ha sido considerada por el Parlamento Europeo, en su informe de 11 de julio de 2000, el instrumento más eficaz para garantizar que la transferencia de datos ofrece las garantías adecuadas. También el Documento del Grupo de Trabajo de Protección de Datos, creado por el artículo 29 de la Directiva Comunitaria, referente a los criterios de interpretación del régimen de transferencias internacionales, de 24 de julio de 1998, contiene previsiones específicas referidas a esta solución contractual.

Por último, la norma sexta se refiere a aquellos casos en que, con independencia del Estado al que se destinen los datos, la transferencia trae causa de la contratación de un

servicio de tratamiento de datos por cuenta del responsable del fichero, transmitiéndose los datos a quien la Ley 15/1999 define como «encargado del tratamiento». En este caso deberá existir, en virtud de lo dispuesto en el artículo 12 de la Ley, y sin perjuicio del cumplimiento de los demás requisitos a los que se refiere la presente Instrucción, un contrato entre las entidades transmitente y destinataria de los datos.

En su virtud, en uso de las facultades que le atribuye el artículo 37 c) de la Ley Orgánica 15/1999, esta Agencia ha dispuesto:

Sección I. Disposiciones generales

Norma primera. *Ámbito de aplicación.*

La presente Instrucción será de aplicación a cualquier supuesto de transferencia internacional de datos de carácter personal.

A tal efecto, se considera transferencia internacional de datos toda transmisión de los mismos fuera del territorio español. En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero.

A los efectos de esta instrucción, se entiende por transmitente la persona física o jurídica, pública o privada, responsable del fichero o tratamiento de los datos de carácter personal que son objeto de transferencia internacional, y por destinatario la persona física o jurídica, pública o privada, situada fuera del territorio español que recibe los datos transferidos.

Norma segunda. *Cumplimiento de las disposiciones de la Ley Orgánica 15/1999.*

La transferencia internacional de datos no excluye de la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, conforme a su ámbito de aplicación, correspondiendo a la Agencia de Protección de Datos la competencia para verificar su cumplimiento.

En todo caso, de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 15/1999, cualquier responsable de un fichero o tratamiento que se proponga transferir datos de carácter personal fuera del territorio español deberá haber informado a los afectados de quiénes serán destinatarios de los datos, así como de la finalidad que justifica la transferencia internacional y el uso de los datos que podrá hacer el destinatario.

El deber de información al que se refiere el párrafo anterior no será de aplicación cuando la transferencia tenga por objeto la prestación de un servicio al responsable del fichero, en los términos establecidos por el artículo 12 de la Ley Orgánica 15/1999.

Norma tercera. *Notificación de las transferencias previstas al Registro General de Protección de Datos.*

1. De conformidad con el artículo 26.2 de la Ley Orgánica 15/1999 cualquier persona o entidad que pretenda efectuar una transferencia internacional de datos deberá hacerlo constar expresamente al proceder a la notificación del fichero al Registro General de Protección de Datos.

La notificación de la transferencia se efectuará en los términos que se contengan en el modelo normalizado aprobado a tal efecto por el Director de la Agencia de Protección de Datos, con expresa indicación del país al que se pretende efectuar la transferencia y de los motivos que, en su caso, la habilitan, conforme a lo dispuesto en el artículo 34 de la citada Ley Orgánica, para no recabar la autorización expresa del Director de la Agencia de Protección de Datos.

En caso de que la transferencia internacional se refiera a datos contenidos en un fichero ya inscrito en el Registro General de Protección de Datos, no constando la transferencia en la inscripción, el responsable del fichero deberá solicitar una modificación de la misma, notificando los extremos a los que se refiere el párrafo anterior.

Si se tratara de ficheros de titularidad pública, la transferencia deberá estar prevista en la norma de creación o modificación del fichero.

2. Recibida la notificación, la Agencia de Protección de Datos podrá requerir al responsable del fichero para que en el plazo de diez días aporte la documentación necesaria para completar la información relativa a la trasferencia internacional contenida en aquélla, así como la identidad del receptor de la misma.

A tal efecto, podrá solicitarse del responsable del fichero o tratamiento que aporte la documentación que acredite el cumplimiento de la obligación a la que se refiere la norma segunda de esta Instrucción. En particular, si el responsable invocase la existencia de consentimiento del afectado a la transferencia, podrá solicitarse que acredite la prestación de ese consentimiento. Del mismo modo podrá exigirse que se acredite la existencia de una relación contractual con el afectado que motive la transferencia, si aquélla hubiera sido alegada.

Igualmente, se podrá solicitar del responsable del fichero que acredite los extremos a los que se refiere la Sección Segunda de la presente Instrucción.

Al requerirse la información a la que se refiere este apartado se indicará al responsable del fichero que, en caso de no ser aquélla aportada en el plazo de diez días, se le tendrá por desistido de su petición de inscripción o modificación, archivándose ésta.

3. Si con la documentación aportada no se acreditara el cumplimiento de los requisitos contenidos en la Ley Orgánica 15/1999, el Director de lasAgencia de Protección de Datos, en ejercicio de las competencias que le atribuye dicha Ley Orgánica, denegará la Inscripción o su modificación.

4. Contra las resoluciones del Director de la Agencia de Protección de Datos relativas a la inscripción o, en su caso, a la modificación de un fichero, cabrá interponer potestativamente recurso previo de reposición o recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.

Sección II. Disposiciones aplicables a transferencias concretas

Norma cuarta. *Transferencias al territorio de Estados que otorguen un nivel adecuado de protección.*

1. Cuando la transferencia internacional tenga por destinatario una persona o entidad, pública o privada, situada en el territorio de un Estado no miembro de la Unión Europea, respecto del que se haya declarado la existencia de un nivel adecuado de protección o que sea miembro del Espacio Económico Europeo, se podrá requerir al responsable del fichero la aportación de la documentación a la que se refiere el apartado segundo de la norma tercera de esta Instrucción.

2. Sin perjuicio de lo dispuesto en la norma segunda, el Director de la Agencia de Protección de Datos, en uso de la potestad que le otorga el artículo 37 f) de la Ley Orgánica 15/1999, podrá acordar, previa audiencia del transmitente, la suspensión temporal de la transferencia de datos hacia un receptor ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes, previstas en las Decisiones de la Comisión de las Comunidades Europeas:

a) Que las Autoridades de Protección de Datos del Estado destinatario o cualquier otra, en caso de no existir las primeras, resuelvan que el destinatario ha vulnerado las normas de protección de datos de su derecho interno.

b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad destinataria de la transferencia y que las autoridades competentes en el Estado en que se encuentre el destinatario no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

En estos casos, la decisión del Director de la Agencia de Protección de Datos será notificada a la Comisión de las Comunidades Europeas.

3. Si la transferencia se funda en lo establecido en la Decisión 2000/520/CE de la Comisión de las Comunidades Europeas, «sobre la adecuación de la protección conferida

por los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos», quien pretenda efectuar la transferencia deberá acreditar que el destinatario se encuentra entre las entidades que se han adherido a los principios, así como que el mismo se encuentra sujeto a la jurisdicción de uno de los organismos públicos estadounidenses que figuran en el Anexo VII de la citada Decisión.

4. Lo indicado en el apartado anterior será de aplicación a todos los supuestos en que el nivel de protección adecuado se declare por la Comisión de las Comunidades Europeas en relación con un sistema de autorregulación o de condiciones similares a las contenidas en la Decisión 2000/520/CE.

5. Contra las resoluciones del Director de la Agencia de Protección de Datos a las que se refiere esta norma cabrá interponer potestativamente recurso previo de reposición o recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.

Norma quinta. *Transferencias al territorio de otros Estados.*

1. Cuando la transferencia internacional tenga por destinatario una persona física o jurídica, pública o privada, situada en el territorio de un Estado no miembro de la Unión Europea, respecto del que no se haya declarado por la Comisión de las Comunidades Europeas la existencia de un nivel adecuado de protección o que no pertenezca al Espacio Económico Europeo y el transmitente se funde en alguno de los supuestos comprendidos en los apartados a) a j) del artículo 34 de la Ley Orgánica 15/1999, la Agencia de Protección de Datos podrá requerir al responsable del fichero para que aporte la documentación que justifique su alegación.

2. En caso de que la transferencia no se fundamente en alguno de los supuestos a los que se refiere el apartado anterior, o cuando esta circunstancia no haya quedado debidamente acreditada, será necesario recabar la autorización del Director de la Agencia de Protección de Datos, conforme a lo dispuesto en el artículo 33 de la Ley Orgánica 15/1999.

Sin perjuicio de lo establecido en el apartado 7 de esta norma, dicha autorización será otorgada en caso de que el responsable del fichero aporte un contrato escrito, celebrado entre el transmitente y el destinatario, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

El citado contrato deberá contener, al menos, las siguientes menciones:

a) La identificación del transmitente y el destinatario de los datos.

b) La indicación de la finalidad que justifica la transferencia internacional, así como de los datos que son objeto de la transferencia.

c) El compromiso del transmitente de que la recogida y tratamiento de los datos en territorio español respeta íntegramente las normas contenidas en la Ley Orgánica 15/1999 y que el fichero en que se encuentran los datos objeto de la transferencia está inscrito en el Registro General de Protección de Datos o se ha solicitado su inscripción.

d) El compromiso del destinatario de que los datos recibidos serán tratados exclusivamente para la finalidad que motiva la transferencia, así como que procederá a su tratamiento de acuerdo con las normas de protección de datos del derecho español. Asimismo, el destinatario deberá comprometerse a no comunicar los datos a ningún tercero en tanto no haya sido recabado el consentimiento del afectado para ello.

e) Que el destinatario adoptará las medidas de seguridad requeridas por la normativa de protección de datos de carácter personal vigente en España.

f) Que el transmitente y el destinatario responderán solidariamente frente a los particulares, a la Agencia de Protección de Datos y a los Órganos Jurisdiccionales españoles por los eventuales incumplimientos del contrato en que pudiera incurrir el receptor, cuando los mismos sean constitutivos de infracción de lo dispuesto en la Ley Orgánica 15/1999 o produzcan un perjuicio a los afectados.

g) Que se indemnizará al afectado que resulte perjudicado como consecuencia del tratamiento efectuado por el destinatario, según el régimen de responsabilidad al que se refiere el apartado anterior.

h) La garantía de que el afectado podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición, tanto ante el transmitente como ante el destinatario de los datos. Asimismo, deberá indicarse que el interesado podrá recabar la tutela de la Agencia de Protección de Datos en los supuestos previstos en la Ley Orgánica 15/1999 en caso de que sus derechos no sean atendidos.

i) El compromiso del destinatario de los datos de autorizar el acceso al establecimiento donde se estén tratando los mismos, así como a la documentación y a los equipos físicos y lógicos, de representantes de la Agencia de Protección de Datos o de la entidad independiente en quien ésta delegue, cuando la Agencia lo requiera con el fin de verificar el cumplimiento de las obligaciones derivadas del contrato.

j) La obligación de que, una vez extinguida la relación contractual, los datos de carácter personal deberán ser destruidos o devueltos al transmitente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transferencia.

k) Que los afectados podrán exigir el cumplimiento de lo estipulado en el contrato en todas aquellas cuestiones en que el mismo les resulte beneficioso.

3. Remitido el contrato, la Agencia de Protección de Datos podrá solicitar que en el mismo se introduzcan las modificaciones necesarias para garantizar el cumplimiento de los requisitos a los que se refieren los dos apartados anteriores, concediendo a tal efecto un plazo de diez días.

4. Transcurrido ese plazo sin que el contrato cumpla los requisitos previstos en los apartados 2 y 3 de esta norma, el Director de la Agencia de Protección de Datos denegará la transferencia solicitada.

5. Cuando el Director de la Agencia de Protección de Datos autorice la transferencia ordenará su inscripción en el Registro General de Protección de Datos y procederá a su comunicación a la Comisión de las Comunidades Europeas.

6. Surtirán el mismo efecto jurídico los contratos que pudieran celebrarse en el futuro al amparo de lo que, en su caso, dispongan las Decisiones de la Comisión de las Comunidades Europeas que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE, siempre que se acredite su íntegro cumplimiento.

7. Sin perjuicio de lo dispuesto en los apartados anteriores de esta norma y en la norma segunda, el Director de la Agencia de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37 f) de la Ley Orgánica 15/1999, suspender temporalmente, previa audiencia del transmitente, la transferencia, cuando concurra alguna de las circunstancias siguientes:

a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.

b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.

c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el destinatario.

d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.

e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

Las resoluciones del Director de la Agencia de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas a las que se refiere este apartado serán notificadas a la Comisión de las Comunidades Europeas cuando así sea exigible.

8. Contra las resoluciones del Director de la Agencia de Protección de Datos cabrá interponer potestativamente recurso previo de reposición o recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.

Norma sexta. *Especialidades en las transferencias que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero.*

1. Cuando la transferencia internacional de datos tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero, la realización del tratamiento deberá estar regulada en un contrato, en que deberá hacerse constar la responsabilidad directa de la transmitente como consecuencia de cualquier incumplimiento de la Ley en que incurriera el destinatario.

El contrato, que deberá constar por escrito, establecerá expresamente que el destinatario únicamente tratará los datos conforme a las instrucciones del transmitente, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato y que adoptará las medidas de seguridad exigibles al transmitente conforme a las normas de protección de datos del Derecho español.

Además, deberá indicarse que una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al transmitente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento

2. La receptora no podrá comunicar los datos, ni siquiera para su conservación, a otras personas.

En consecuencia, si la transmitente deseara que por parte de varias entidades distintas, situadas fuera del territorio español, se presten servicios de tratamiento, en los términos a que se refiere el artículo 12 de la Ley Orgánica 15/1999, deberá contratar dichos servicios con cada una de las entidades, no siendo posible que la destinataria subcontrate esta segunda actividad con otra empresa, a menos que actúe en nombre y por cuenta del responsable del fichero.

3. En caso de que la transferencia se dirija a un destinatario situado en un Estado no miembro de la Unión Europea respecto del que no se haya declarado la existencia de un nivel adecuado de protección o que no pertenezca al Espacio Económico Europeo, en el contrato deberán constar cautelas semejantes a las indicadas en la norma quinta en lo referente al régimen sancionador y de indemnización a los interesados, así como en lo relativo a las potestades de la Agencia de Protección de Datos, para el caso en que la destinataria emplee los datos para otra finalidad distinta de la que motivó la transferencia, los comunique o los utilice incumpliendo las estipulaciones del contrato.

§ 18

Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo

Agencia de Protección de Datos
«BOE» núm. 62, de 12 de marzo de 1996
Última modificación: sin modificaciones
Referencia: BOE-A-1996-5698

La necesidad de establecer la forma de llevar los ficheros automatizados utilizados para controlar la entrada en casinos y salas de bingo obliga a precisar una serie de criterios interpretativos que faciliten la aplicación de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, con mayor razón desde la aprobación de la Directiva europea relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En concreto, es necesario regular el cumplimiento del deber de información al ciudadano en la recogida de datos personales, el consentimiento en la cesión de los datos así recabados en los supuestos en que la misma no debe efectuarse por causas legales, así como el plazo en que los datos deben ser cancelados por haber dejado de ser necesarios o pertinentes para los fines para los que se recabaron.

La Instrucción solamente se refiere al ámbito competencial propio de la Ley reguladora del tratamiento automatizado de datos personales y se dicta de conformidad con lo dispuesto en el artículo 36.c) de la misma que atribuye a la Agencia de Protección de Datos competencias en esta materia.

Norma primera. *Ámbito de aplicación.*

1. La presente Instrucción regula los datos de carácter personal tratados de forma automatizada que son recabados con la finalidad de controlar el acceso por las sociedades explotadoras de casinos de juego o por cualquier empresa titular de una sala de bingo.

2. A tales efectos, tendrá la consideración de dato personal cualquier información concerniente a personas físicas identificadas o identificables, debiendo entenderse comprendidos dentro de la misma el sonido y la imagen.

Norma segunda. *Responsable del fichero.*

1. Tendrá la consideración de responsable del fichero la sociedad explotadora del casino de juego o la empresa titular de la sala de bingo.

2. El responsable del fichero asumirá el cumplimiento de todas las obligaciones establecidas en la Ley Orgánica 5/1992 y, entre ellas, la de la inscripción del fichero en el Registro General de Protección de Datos.

Norma tercera. *Recogida de datos.*

1. La recogida de datos efectuada para el cumplimiento de los fines a los que se refiere la presente Instrucción deberá realizarse de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 5/1992, y, en concreto, deberá informarse de la existencia de un fichero automatizado, de la finalidad de la recogida de datos, de los destinatarios de la información, del carácter obligatorio de su respuesta, de las consecuencias de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación o cancelación y de la identidad y dirección del responsable del fichero.

2. No podrán recogerse más datos personales que aquellos estrictamente necesarios para controlar el acceso, quedando, en todo caso, limitados a los que aparecen en el documento identificador exigido para la entrada.

Norma cuarta. *Utilización de los datos.*

Los datos personales así obtenidos no podrán ser utilizados para otros fines. Tampoco podrán ser objeto de cesión los datos así recabados fuera de los casos expresamente establecidos en la ley, salvo consentimiento del afectado.

Norma quinta. *Cancelación de los datos.*

Los datos de carácter personal deberán ser destruidos cuando haya transcurrido el plazo de seis meses, contado a partir de la fecha del último acceso.

Norma sexta. *Medidas de seguridad.*

El responsable del fichero garantizará la adopción de las medidas técnicas y organizativas necesarias para la seguridad de los datos y que impidan el acceso no autorizado a los ficheros creados para dichos fines.

Norma final. *Entrada en vigor.*

La presente Instrucción entrará en vigor a partir de los tres meses de su publicación en el «Boletín Oficial del Estado».

§ 19

Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación

Agencia de Protección de Datos
«BOE» núm. 25, de 29 de enero de 1998
Última modificación: sin modificaciones
Referencia: BOE-A-1998-1943

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, dedica los artículos 14 y siguientes a los derechos de acceso, rectificación y cancelación de los datos de carácter personal contenidos en ficheros automatizados. Dichos derechos se configuran como uno de los ejes fundamentales sobre los que se articula la protección del honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, en desarrollo de lo dispuesto en el artículo 18.4 de la Constitución Española.

El ejercicio de los derechos de acceso, rectificación y cancelación aparece regulado no sólo en la Ley Orgánica 5/1992, sino también en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos procedimentales de la citada Ley.

Al amparo de lo dispuesto en el artículo 36.c) de la Ley Orgánica 5/1992 que atribuye al Director de la Agencia la función de «dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la presente Ley», se ha elaborado la presente Instrucción.

Esta Instrucción tiene por objeto aclarar las disposiciones relativas a los derechos de acceso, rectificación y cancelación, ya que las actuaciones practicadas por esta Agencia han puesto de manifiesto que en su aplicación se presentan problemas interpretativos y que es necesario precisar el ejercicio de estos derechos en relación con algunos ficheros que presentan características especiales. Para ello, la Instrucción recoge la regulación de dichos derechos de acuerdo con la Ley Orgánica 5/1992 y el Real Decreto 1332/1994, de 20 de junio, y realiza una interpretación unitaria de los preceptos teniendo en cuenta la totalidad de principios legales.

En las normas primera, segunda y tercera se detallan los requisitos que deben cumplirse en el ejercicio de los derechos de acceso, rectificación y cancelación con carácter general. Sin embargo, las particularidades que presentan los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito y los ficheros con fines de publicidad exigen tratarlos de un modo especial en las normas cuarta y quinta, respectivamente.

Norma primera. *Requisitos generales.*

1. Los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos y serán ejercidos por el afectado frente al responsable del fichero por lo que será necesario que el afectado acredite su identidad frente

a dicho responsable. Estos derechos se ejercerán sin otras limitaciones que las que prevén la Ley Orgánica 5/1992 y el Real Decreto 1332/1994, de 20 de junio.

Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos, en cuyo caso será necesario que el representante legal acredite tal condición.

2. La Ley configura los derechos de acceso, rectificación y cancelación como derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

3. El ejercicio de los derechos deberá llevarse a cabo mediante solicitud dirigida al responsable del fichero, que contendrá:

Nombre, apellidos del interesado y fotocopia del documento nacional de identidad del interesado y, en los casos que excepcionalmente se admita, de la persona que lo represente, así como el documento acreditativo de tal representación. La fotocopia del documento nacional de identidad podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido en derecho.

Petición en que se concreta la solicitud.

Domicilio a efectos de notificaciones, fecha y firma del solicitante.

Documentos acreditativos de la petición que formula, en su caso.

El interesado deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.

4. El responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción.

En el caso de que la solicitud no reúna los requisitos especificados en el apartado tercero, el responsable del fichero deberá solicitar la subsanación de los mismos.

5. El responsable del fichero deberá adoptar las medidas oportunas para garantizar que todas las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

Norma segunda. *Derecho de acceso.*

1. El afectado tiene derecho a solicitar y obtener información de sus datos de carácter personal incluidos en ficheros automatizados.

2. Al ejercitar el derecho de acceso, el afectado podrá optar por uno o varios de los siguientes sistemas de consulta del fichero, siempre que la configuración o implantación material del fichero lo permita:

a) Visualización en pantalla.

b) Escrito, copia o fotocopia remitida por correo.

c) Telecopia.

d) Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo.

3. El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

4. Si la resolución fuera estimatoria, el acceso se hará efectivo en el plazo de los diez días siguientes a la notificación de aquélla.

5. El responsable del fichero podrá denegar el acceso a los datos de carácter personal cuando el derecho se haya ejercitado en un intervalo inferior a doce meses y no se acredite un interés legítimo al efecto, así como cuando la solicitud sea formulada por persona distinta del afectado.

Tratándose de ficheros de titularidad pública se podrá denegar el acceso en los supuestos de los artículos 21.1 y 21.2 de la Ley Orgánica 5/1992, en los que se establecen

excepciones relativas a los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado y a los ficheros de la Hacienda Pública y del artículo 22 de la Ley Orgánica 5/1992.

6. La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, previa transcripción en claro de los datos del fichero, en su caso, y comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

En el caso de que los datos provengan de fuentes diversas, deberán especificarse las mismas identificando la información que proviene de cada una de ellas.

Norma tercera. *Derechos de rectificación y cancelación.*

1. Si los datos de carácter personal del afectado son inexactos o incompletos, inadecuados o excesivos, podrá éste solicitar del responsable del fichero la rectificación o, en su caso, la cancelación de los mismos.

2. Los derechos de rectificación y cancelación se harán efectivos por el responsable del fichero dentro de los cinco días siguientes al de la recepción de la solicitud. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, a su vez, la lleve a cabo en su fichero.

3. La solicitud de rectificación deberá indicar el dato que es erróneo y la corrección que debe realizarse y deberá ir acompañada de la documentación justificativa de la rectificación solicitada, salvo que la misma dependa exclusivamente del consentimiento del interesado.

4. En la solicitud de cancelación, el interesado deberá indicar si revoca el consentimiento otorgado, en los casos en que la revocación proceda, o si, por el contrario, se trata de un dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa.

5. La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos.

6. Si solicitada la rectificación o cancelación, el responsable del fichero considera que no procede atender la solicitud del afectado, se lo comunicará motivadamente dentro del plazo de los cinco días siguientes al de la recepción de la misma, a fin de que por éste se pueda hacer uso de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992.

7. Transcurrido el plazo de cinco días sin que de forma expresa se responda a la solicitud de rectificación o cancelación, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación que corresponda.

8. La cancelación exige el borrado físico de los datos, sin que sea suficiente a estos efectos una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren las bajas producidas.

9. En los casos en que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el responsable del fichero procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización.

Se exceptúa, no obstante, el supuesto en el que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.

Norma cuarta. *Ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito.*

1. El ejercicio de los derechos de acceso, rectificación y cancelación en el caso de los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito se rige por las normas anteriores de la presente Instrucción, sin perjuicio de lo señalado en los apartados siguientes.

2. El responsable de un fichero de prestación de servicios de solvencia patrimonial y crédito con datos obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento, estará obligado a satisfacer, en cualquier caso, los derechos de acceso, rectificación y cancelación. Las personas y entidades a las

que se presta el servicio únicamente estarán obligadas a comunicar al afectado aquellos datos relativos al mismo a los que ellas tengan acceso y a comunicar la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

3. El responsable del fichero común en el que se traten automatizadamente datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés, ante una solicitud de ejercicio del derecho de acceso, deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero. Cualquier otra entidad participante en el sistema, ante tal solicitud, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad del responsable del fichero común para que pueda completar el ejercicio de su derecho de acceso.

Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige al responsable del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de cinco días, procederá a la rectificación o cancelación cautelar de los mismos.

Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige a cualquier otra entidad participante en el sistema y hace referencia a datos que dicha entidad haya facilitado al fichero común, procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al responsable del fichero común en el plazo de cinco días. Si la solicitud hace referencia a datos que la entidad no hubiera facilitado al fichero común, dicha entidad informará al afectado sobre este hecho, proporcionándole, además, la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

4. En los ficheros de prestación de servicios de información de solvencia patrimonial y crédito, cualquiera que sea el origen de los datos, cuando el afectado lo solicite el responsable del fichero común deberá cumplir la obligación establecida en el artículo 28.2 de la Ley Orgánica 5/1992 de facilitar, las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.

Norma quinta. *Ficheros con fines de publicidad.*

1. El responsable del fichero que presta el servicio de publicidad estará obligado a satisfacer los derechos de acceso, rectificación y cancelación. La entidad beneficiaria de la publicidad estará obligada a indicar al afectado la identidad del responsable del fichero del que provienen los datos. A tal efecto, se entenderá suficiente que dicha información se haga constar en la campaña publicitaria.

2. Cuando el interesado manifieste su deseo de no recibir publicidad, y no ejerza expresamente el derecho de cancelación, el responsable del fichero podrá conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

Disposición final única.

La presente Instrucción entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

§ 20

Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios

Agencia de Protección de Datos
«BOE» núm. 62, de 12 de marzo de 1996
Última modificación: sin modificaciones
Referencia: BOE-A-1996-5697

La necesidad de regular los ficheros automatizados establecidos para el control del acceso de las personas a los centros de trabajo o dependencias públicas, a donde se acude con la finalidad de efectuar actividades relacionadas con las propias del centro visitado, plantea problemas relacionados con la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, con mayor razón desde la aprobación de la Directiva europea relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Estos problemas se concretan en la necesidad de regular los datos constituidos por sonido e imagen, como los de vigilancia por videocámara, y, en general, todos los recopilados en cumplimiento de las funciones de vigilancia, con la prestación del consentimiento necesario para ello, así como el período en que los mismos deban ser conservados y su posterior cancelación por haber dejado de ser necesarios o pertinentes para los fines para los que fueron recabados.

La Instrucción solamente se refiere al ámbito competencial propio de la Ley reguladora del tratamiento automatizado de datos personales y se dicta de conformidad con lo dispuesto en el artículo 36.c) de la misma que atribuye a la Agencia de Protección de Datos competencias en esta materia.

Norma primera. *Ámbito de aplicación.*

1. La presente Instrucción regula los datos de carácter personal tratados de forma automatizada que son recabados por los servicios de seguridad con la finalidad de controlar el acceso a los edificios públicos y privados, así como a establecimientos, espectáculos, certámenes y convenciones.

2. A tales efectos, tendrá la consideración de dato personal cualquier información concerniente a personas físicas identificadas o identificables, debiendo entenderse comprendidos dentro de la misma el sonido y la imagen.

Norma segunda. *Responsable del fichero.*

1. Tendrá la consideración de responsable del fichero la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo por cuya cuenta se efectúe la realización del servicio de seguridad. No obstante lo anterior, mediante el correspondiente

contrato de prestación de servicios de seguridad, podrá tener la consideración de responsable del fichero la empresa que preste los servicios de aquella naturaleza.

2. El responsable del fichero asumirá el cumplimiento de todas las obligaciones establecidas en la Ley Orgánica 5/1992 y, entre ellas, la de la inscripción del fichero en el Registro General de Protección de Datos.

Norma tercera. *Recogida de datos.*

1. La recogida de datos efectuada para el cumplimiento de los fines a los que se refiere la presente Instrucción deberá realizarse de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 5/1992, y, en concreto, deberá informarse de la existencia de un fichero automatizado, de la finalidad de la recogida de los datos, de los destinatarios de la información, del carácter obligatorio de su respuesta, de las consecuencias de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación o cancelación y de la identidad y dirección del responsable del fichero.

2. Los datos recogidos serán los estrictamente necesarios para cumplir la finalidad de controlar el acceso.

Norma cuarta. *Utilización de los datos.*

Los datos personales así obtenidos no podrán ser utilizados para otros fines. Tampoco podrán ser objeto de cesión los datos así recabados fuera de los casos expresamente establecidos en la ley, salvo consentimiento del afectado.

Norma quinta. *Cancelación de los datos.*

Los datos de carácter personal deberán ser destruidos cuando haya transcurrido el plazo de un mes, contado a partir del momento en que fueron recabados.

Norma sexta. *Medidas de seguridad.*

El responsable del fichero garantizará la adopción de las medidas técnicas y organizativas necesarias para la seguridad de los datos y que impidan el acceso no autorizado a los ficheros creados para dichos fines.

Norma final. *Entrada en vigor.*

La presente Instrucción entrará en vigor a partir de los tres meses de su publicación en el «Boletín Oficial del Estado».

§ 21

Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal

Agencia de Protección de Datos
«BOE» núm. 110, de 9 de mayo de 1995
Última modificación: sin modificaciones
Referencia: BOE-A-1995-10931

La concesión de un crédito hipotecario o personal, que suele ir acompañada de un seguro de vida por el importe de aquél y del que se señala como beneficiaria a la entidad de crédito de que se trate por la suma del capital no amortizado, incide sobre un importante número de disposiciones de nuestro ordenamiento jurídico.

Es obvio que la regulación jurídica de alguna de estas materias (Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios; Ley 16/1989, de 17 de julio, de Defensa de la Competencia; Ley 9/1992, de 30 de abril, de Mediación en Seguros Privados), excede de las competencias que tiene atribuidas la Agencia de Protección de Datos. Ahora bien, la precisión de si los datos son o no sensibles, con la incidencia que ello tiene en su recogida, tratamiento y cesión, la determinación del fichero en donde deban ser tratados, la de si es preciso que en esta materia, por tratarse de datos especialmente protegidos, el nivel de protección de los mismos se extienda excepcionalmente a los ficheros manuales o no automatizados, son, entre otras, cuestiones que deben ser fijadas por la Agencia de Protección de Datos.

En consecuencia, en uso de las facultades que tiene conferidas, la Agencia de Protección de Datos ha dispuesto:

Norma primera. *Ámbito de aplicación.*

La presente Instrucción será de aplicación a los datos personales solicitados por las entidades de crédito con motivo de la celebración de un contrato de seguro de vida anejo a la concesión de un crédito hipotecario o personal.

Norma segunda. *De la recogida de los datos.*

1. La obtención de datos personales a efectos de la celebración de un contrato de seguro de vida, anejo a la concesión de un crédito hipotecario o personal, efectuada por las entidades de crédito a través de cuestionarios u otros impresos deberá realizarse, en todo caso, mediante modelos separados para cada uno de los contratos a celebrar. En los formularios cuyo destinatario sean las entidades bancarias no podrán recabarse en ningún caso datos relativos a la salud del solicitante.

2. Cualquiera que sea el modo de llevarse a efecto la recogida de datos de salud necesarios para la celebración del seguro de vida deberá constar expresamente el compromiso de la entidad de crédito de que los datos obtenidos a tal fin solamente serán utilizados por la entidad aseguradora. Las entidades de crédito no podrán incluir los datos de salud en sus ficheros informatizados o en aquéllos en los que almacenen datos de forma convencional.

3. En ningún caso se considerará, por la naturaleza de la información solicitada o por las circunstancias en que se recaba, que se puede prescindir del derecho de la información en la recogida de los datos previstos en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Por tanto, será necesario informar previamente, en los formularios u otros impresos de recogida, de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

e) De la identidad y dirección del responsable del fichero.

4. Cuando la recogida de datos personales a efectos de la celebración de un contrato de seguro de vida, anejo a la concesión de un crédito hipotecario o personal efectuada por las entidades de crédito, se lleve a cabo por procedimientos distintos a los del formulario u otros impresos deberá informarse al afectado de los extremos previstos en el apartado tercero.

Norma tercera. *Consentimiento del afectado y tratamiento de los datos.*

El afectado deberá manifestar su consentimiento por separado para cada uno de los contratos y para el tratamiento distinto de la información que ambos conllevan.

Las entidades de crédito solamente podrán tratar aquellos datos personales, no especialmente protegidos, que sean estrictamente necesarios para relacionar el contrato de préstamo con el contrato de seguro de vida celebrado como consecuencia de aquél o que estén justificados por la intervención de la entidad de crédito como agente o tomador del contrato de seguro.

Norma cuarta. *Cesión de los datos.*

En ningún caso podrá considerarse que la cesión de cualquier clase de datos personales solicitados por la entidad aseguradora a la de crédito, o viceversa, se halla amparada por lo establecido en el artículo 11.2. c), de la Ley Orgánica 5/1992.

Norma transitoria. *Aplicación a contratos celebrados con anterioridad.*

Los datos de salud correspondientes a los contratos de seguro de vida celebrados con anterioridad a la publicación de esta Instrucción, que se encuentren incluidos en ficheros de las entidades de crédito, automatizados o no, deberán ser cancelados en el plazo de un mes, contado a partir de la entrada en vigor de la misma.

Norma final. *Entrada en vigor.*

La presente Instrucción entrará en vigor al día siguiente de su publicación en el «Boletín Oficial del Estado».

§ 22

Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito

Agencia de Protección de Datos
«BOE» núm. 54, de 4 de marzo de 1995
Última modificación: sin modificaciones
Referencia: BOE-A-1995-5746

El artículo 36 de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, al definir las funciones de la Agencia de Protección de Datos, incluye en su apartado c) la de dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de dicha Ley. Disposición que tiene su complemento en el artículo 5.c) del Estatuto de la Agencia, aprobado por Real Decreto 428/1993, de 26 de marzo, que señala entre las funciones de la misma la de dictar las instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica.

El artículo 28 de la misma se refiere a la prestación de servicios de información sobre solvencia patrimonial y crédito desde una doble perspectiva. Por un lado, determina que quienes se dediquen a la prestación de servicios sobre la solvencia patrimonial y el crédito sólo podrán tratar automatizadamente datos de carácter personal obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento. Por otro, regula el tratamiento de datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias señalando que podrán tratarse dichos datos siempre que sean «facilitados por el acreedor o por quien actúe por su cuenta o interés».

Los primeros no se apartan de la regulación común que establece la Ley Orgánica; los segundos presentan, por el contrario, un conjunto de especialidades (excepción del principio del consentimiento tanto en la recogida del dato como en su tratamiento), que hacen necesario efectuar una serie de precisiones. Además, dentro de estos últimos, la realidad demuestra que coexisten perfectamente engarzados dos tipos de ficheros: Uno, el propio del acreedor, que se nutre de los datos personales que son consecuencia de las relaciones económicas mantenidas con el afectado, cuya única finalidad es obtener la satisfacción de la obligación dineraria, y otro, un fichero que se podría denominar común que, consolidando todos los datos personales contenidos en aquellos otros ficheros, tiene por finalidad proporcionar información sobre la solvencia de una persona determinada y cuyo responsable, al no ser el acreedor, no tiene competencia para modificar o cancelar los datos inexactos que se encuentran en aquéllos.

En consecuencia, en uso de las facultades que tiene conferidas, la Agencia de Protección de Datos ha dispuesto:

CAPÍTULO I

Calidad de los datos objeto del tratamiento automatizado, forma y veces en que debe efectuarse la notificación y cómputo del plazo al que se refiere el artículo 28.3 de la Ley Orgánica

Norma primera. *Calidad de los datos objeto de tratamiento.*

1. La inclusión de los datos de carácter personal en los ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias, a los que se refiere el artículo 28 de la Ley Orgánica 5/1992, deberá efectuarse solamente cuando concurran los siguientes requisitos:

a) Existencia previa de una deuda cierta, vencida y exigible, que haya resultado impagada.
b) Requerimiento previo de pago a quien corresponda, en su caso, el cumplimiento de la obligación.

2. No podrán incluirse en los ficheros de esta naturaleza datos personales sobre los que exista un principio de prueba documental que aparentemente contradiga alguno de los requisitos anteriores. Tal circunstancia determinará igualmente la desaparición cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado su inclusión en el fichero.
3. El acreedor o quien actúe por su cuenta e interés deberá asegurarse que concurren todos los requisitos exigidos en el número 1 de esta norma en el momento de notificar los datos adversos al responsable del fichero común.
4. La comunicación del dato inexistente o inexacto, con el fin de obtener su cancelación o modificación, deberá efectuarse por el acreedor o quien actúe por su cuenta al responsable del fichero común en el mínimo tiempo posible, y en todo caso en una semana. Dicho plazo es independiente del establecido en el artículo 15.2 del Real Decreto 1332/1994, de 20 de junio, y que se aplica al fichero del acreedor.

Norma segunda. *Notificación de la inclusión en el fichero.*

1. La notificación de la inclusión de datos personales en el fichero efectuada con posterioridad a la entrada en vigor de la Ley Orgánica 5/1992 se efectuará en la forma establecida en el artículo 28 de la misma.
2. Cuando se trate de datos personales incorporados al fichero con anterioridad a la entrada en vigor de la Ley Orgánica deberán notificarse al afectado en el menor plazo posible y, en todo caso, dentro del año siguiente contado desde la publicación de la presente Instrucción.
3. La inscripción en el fichero de la obligación incumplida se efectuará, bien en un solo asiento si fuese de vencimiento único, bien en tantos asientos como vencimientos periódicos incumplidos existan señalando, en este caso, la fecha de cada uno de ellos.
4. Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.
5. El responsable del fichero deberá adoptar las medidas organizativas y técnicas necesarias que permitan acreditar la realización material del envío de notificación y la fecha de entrega o intento de entrega de la misma.
6. La notificación se dirigirá a la última dirección conocida del afectado a través de un medio fiable e independiente del responsable del fichero.

Norma tercera. *Cómputo del plazo de seis años que establece el artículo 28.3 de la Ley Orgánica.*

El cómputo del plazo a que se refiere el artículo 28.3 de la Ley Orgánica se iniciará a partir del momento de la inclusión del dato personal desfavorable en el fichero y, en todo caso, desde el cuarto mes, contado a partir del vencimiento de la obligación incumplida o del plazo en concreto de la misma si fuera de cumplimiento periódico.

CAPITULO II

Medidas de seguridad

Norma cuarta. *Forma de comprobación.*

1. Los sistemas que almacenen o procesen información relativa al cumplimiento o incumplimiento de obligaciones dinerarias deberán acreditar la efectiva implantación de las medidas de seguridad exigidas por el artículo 9.1 de la Ley Orgánica dentro del año siguiente a la publicación de la presente Instrucción. Para los ficheros que se inscriban con posterioridad a esta Instrucción, el plazo se computará a partir de la fecha en que aquélla se haya efectuado en el Registro General de Protección de Datos.

2. La implantación, idoneidad y eficacia de dichas medidas se acreditará mediante la realización de una auditoría, proporcionada a la naturaleza, volumen y características de los datos personales almacenados y tratados, y la remisión del informe final de la misma a la Agencia de Protección de Datos.

3. La auditoría podrá ser realizada:

a) Por el departamento de auditoría interna del responsable del fichero, si cuenta con un departamento formalmente constituido, profesionalmente cualificado e independiente del órgano responsable del tratamiento y gestión de los datos.

b) Por un auditor externo, profesionalmente cualificado e independiente del responsable del fichero.

4. La auditoría deberá ser realizada de acuerdo con las normas y recomendaciones de ejercicio profesional aplicables en el momento de su ejecución.

5. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles destinados a garantizar la integridad y confidencialidad de los datos personales almacenados o tratados, identificar sus deficiencias o insuficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basan los dictámenes alcanzados y recomendaciones propuestas.

6. Adicionalmente, los sistemas que almacenen o procesen información relativa al cumplimiento o incumplimiento de obligaciones dinerarias deberán someterse a una nueva auditoría tras la adopción de las medidas específicas que, en su caso, la Agencia determine, a resultas del informe inicial de auditoría. En todo caso, dichos sistemas deberán ser auditados periódicamente, a intervalos no mayores de dos años.

Norma final. *Entrada en vigor.*

La presente Instrucción entrará en vigor al día siguiente de su publicación en el «Boletín Oficial del Estado».

§ 23

Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos

Comunidad Autónoma del País Vasco
«BOPV» núm. 44, de 4 de marzo de 2004
«BOE» núm. 279, de 19 de noviembre de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-18151

Se hace saber a todos los ciudadanos y ciudadanas de Euskadi que el Parlamento Vasco ha aprobado la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

EXPOSICIÓN DE MOTIVOS

Los avances de la técnica se han acelerado en los últimos tiempos. Actualmente, el uso de la informática permite tratar gran cantidad de datos relativos a las personas físicas, pudiendo llegar a conocer aspectos relacionados con las mismas que suponen una intromisión en su intimidad. Los ordenamientos jurídicos no pueden permanecer insensibles ante la eventualidad de usos perversos de las posibilidades tecnológicas, en detrimento de espacios que deben quedar reservados a la intimidad personal.

Esta tensión entre tecnología, especialmente en el campo de la informática, e intimidad de las personas apela a una actuación legislativa que procure un equilibrio satisfactorio entre dos bienes dignos de protección jurídica. Por un lado, no es bueno para la sociedad poner freno al desarrollo tecnológico, cuyas potencialidades son inmensas y deben contribuir a un mayor bienestar de la comunidad; pero, por otro, los ciudadanos tienen derecho a que se les proteja su intimidad personal, evitando que las posibilidades que ofrece la tecnología informática actual reduzcan aquélla más allá de lo deseable. Para ello es preciso limitar el uso de la informática y, de este modo, garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Es éste un mandato que el artículo 18.4 de la Constitución impone al legislador, y que éste recoge en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La preocupación por la protección de la intimidad personal y familiar de los ciudadanos, con la consiguiente limitación del uso de la informática a tal fin, no es exclusiva del legislador estatal. También las instituciones de la Unión Europea han mostrado su sensibilidad en este sentido.

El Tratado de Amsterdam de 17 de junio de 1997 ha incorporado al tratado constitutivo de la Comunidad Europea su actual artículo 286, que requiere que se apliquen a las instituciones y organismos comunitarios los actos comunitarios relativos a la protección de

las personas respecto al tratamiento de datos personales y a la libre circulación de estos datos.

Ya anteriormente, el Parlamento Europeo y el Consejo habían adoptado la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, donde se recoge el principio de que los sistemas de tratamiento de datos están al servicio del hombre y que deben respetar las libertades y derechos fundamentales de las personas físicas, en particular la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios y al bienestar de los individuos.

Según esta directiva, las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los citados derechos y libertades, particularmente el derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho comunitario, y considera que la aproximación de dichas legislaciones debe tener por objeto asegurar un alto nivel de protección.

Para la citada directiva, un elemento esencial de la protección de las personas, en lo que respecta a la protección de los datos personales, es la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros, la cual debe disponer de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención.

La directiva da a los estados miembros un plazo de tres años para la adopción de las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la misma.

La actuación de las instituciones comunitarias en materia de protección de datos no se ha limitado a las directivas destinadas a los estados miembros, sino que también han adoptado medidas destinadas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios, mediante el Reglamento (CE) número 45/2001, del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, el cual incluso instituye una autoridad de control independiente (el Supervisor Europeo de Protección de Datos).

Podría decirse que la garantía de un elevado nivel de protección de los datos personales y de la intimidad es un principio inspirador de la normativa comunitaria, que tiene su proyección incluso en propuestas de directiva cuya finalidad no es propiamente la regulación de la protección de los datos de carácter personal, como es el caso de la propuesta de directiva del Parlamento Europeo y del Consejo relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Diario Oficial núm. C 365 E de 19/12/2000).

En el Derecho interno, la protección de datos de carácter personal se halla regulada, como decíamos antes, en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que, además de otras materias vinculadas con el derecho fundamental al que se refiere el artículo 18.4 de la Constitución, regula los aspectos básicos del régimen jurídico de la Agencia de Protección de Datos, que es la que se configura como la autoridad de control independiente a la que se refiere la Directiva 95/46/CE.

La ley orgánica establece que la mayor parte de las funciones asignadas a la citada agencia, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las comunidades autónomas y por la Administración local de su ámbito territorial, serán ejercidas por los órganos correspondientes de cada comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido. Criterio legal que es acorde con el artículo 28 de la Directiva 95/46/CE, según el cual los estados miembros dispondrán de una o más autoridades públicas que se encargarán de vigilar la aplicación, en su territorio, de las disposiciones adoptadas por ellos de acuerdo con la citada directiva, y añade que dichas autoridades ejercerán las funciones que les son atribuidas con total independencia.

Desde el punto de vista de su ordenación sistemática, la ley se halla dividida en tres títulos.

En el título I, de disposiciones generales, se concretan el objeto y el ámbito de aplicación de la ley, delimitando los ficheros que quedan bajo su regulación atendiendo a la Administración pública, institución o corporación que los crea o gestiona. La citada delimitación se completa con la enumeración de los ficheros a los que no se aplicará la ley y de aquellos en los que ésta será de aplicación limitada, por tener regímenes específicos. Contiene también una lista de definiciones muy útil para precisar y unificar la terminología específica de la materia objeto de regulación; se regulan aspectos relacionados con la creación, modificación y supresión de ficheros, limitaciones a la recogida de datos de carácter personal, información a los interesados y seguridad de los ficheros de datos, así como el procedimiento de reclamación ante la Agencia Vasca de Protección de Datos. Se trata de un título necesario para dar coherencia sistemática e integridad a la ley, que requerirá de un desarrollo posterior.

En el título II se crea la Agencia Vasca de Protección de Datos y se regulan los aspectos fundamentales de su régimen jurídico. Contiene preceptos relativos al régimen del personal a su servicio, recursos económicos, régimen presupuestario, órganos de gobierno, funciones y potestades. Es de resaltar la creación del Registro de Protección de Datos como órgano necesario de la agencia.

El título III está dedicado al régimen sancionador. En él se delimitan los sujetos responsables, se tipifican las infracciones y se establecen las sanciones correspondientes. Como dice el Reglamento (CE) número 45/2001, antes citado, un sistema de protección de datos personales requiere establecer derechos y obligaciones, pero también sanciones apropiadas para los infractores. En nuestro caso, dadas las características especiales de los titulares de los ficheros, se presta especial atención al supuesto de infracciones cometidas por el personal al servicio de las administraciones, instituciones y corporaciones a cuyos ficheros se aplica la ley.

La ley contiene tres disposiciones adicionales, relativas a la necesaria comunicación de los ficheros existentes a la Agencia Vasca de Protección de Datos, a la utilización de los datos del padrón municipal por las administraciones autonómica y forales para el ejercicio de sus competencias, y al necesario respeto de las competencias del Ararteko y de la Agencia de Protección de Datos del Estado.

Concluye con una disposición final, en la que se autoriza al Gobierno Vasco para su desarrollo y aplicación.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

La presente ley tiene por objeto:

1. La regulación de los ficheros de datos de carácter personal creados o gestionados por la Comunidad Autónoma del País Vasco, los órganos forales de los territorios históricos y las administraciones locales de la Comunidad Autónoma del País Vasco.

2. La creación y regulación de la Agencia Vasca de Protección de Datos.

Artículo 2. *Ámbito de aplicación.*

1. La presente ley será aplicable a los ficheros de datos de carácter personal creados o gestionados, para el ejercicio de potestades de derecho público, por:

a) La Administración General de la Comunidad Autónoma, los órganos forales de los territorios históricos y las administraciones locales del ámbito territorial de la Comunidad Autónoma del País Vasco, así como los entes públicos de cualquier tipo, dependientes o vinculados a las respectivas administraciones públicas, en tanto que los mismos hayan sido creados para el ejercicio de potestades de derecho público.

b) El Parlamento Vasco.

c) El Tribunal Vasco de Cuentas Públicas.

d) El Ararteko.

e) El Consejo de Relaciones Laborales.
f) El Consejo Económico y Social.
g) El Consejo Superior de Cooperativas.
h) La Agencia Vasca de Protección de Datos.
i) La Comisión Arbitral.
j) Las corporaciones de derecho público, representativas de intereses económicos y profesionales, de la Comunidad Autónoma del País Vasco.
k) Cualesquiera otros organismos o instituciones, con o sin personalidad jurídica, creados por ley del Parlamento Vasco, salvo que ésta disponga lo contrario.

2. No obstante lo dispuesto en el número anterior, esta ley no será de aplicación a los ficheros:

a) Sometidos a la normativa sobre protección de materias clasificadas.
b) Establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.
c) Regulados por la legislación de régimen electoral.
d) Procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por los cuerpos de Policía del País Vasco, de conformidad con la legislación sobre la materia.

3. Se regirán por sus disposiciones específicas y, en su caso, por lo especialmente previsto en esta ley los tratamientos de datos personales que sirvan a fines exclusivamente estadísticos y estén amparados por la legislación sobre la función estadística pública.
4. Las instituciones y centros sanitarios de carácter público y los profesionales a su servicio podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratadas en los mismos, de acuerdo con lo dispuesto en la legislación sectorial sobre sanidad, sin perjuicio de la aplicación de lo dispuesto en esta ley en todo lo que no sea incompatible con aquella legislación.
5. La aplicación de lo dispuesto en esta ley a los ficheros de datos de carácter personal, distintos de los citados en el número 2 de este artículo, creados o gestionados por los cuerpos de Policía del País Vasco se efectuará sin perjuicio de las especificidades de su régimen jurídico previstas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en la Ley 4/1992, de 17 de julio, de Policía del País Vasco.

Artículo 3. *Definiciones.*

A los efectos de esta ley se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables. Se considerará identificable toda persona cuya identidad pueda determinarse directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.
b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso.
c) Tratamiento de datos: operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
d) Responsable del fichero o tratamiento: persona, institución, entidad, corporación u órgano administrativo al que está adscrito el fichero y que decide sobre la finalidad, contenido y uso del tratamiento. La disposición por la que se cree el fichero determinará el responsable del mismo. Sus funciones serán las establecidas en el documento de seguridad.
e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere la letra c) de este artículo.
f) Encargado del tratamiento: persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

g) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que la conciernen.

h) Cesión o comunicación de datos: toda revelación de datos realizada a persona distinta del interesado.

Artículo 4. *Creación, modificación y supresión de ficheros.*

1. La creación, modificación y supresión de ficheros de la Administración de la Comunidad Autónoma se realizará por orden del titular del departamento al que esté adscrito el fichero, la cual deberá contener todas las menciones exigidas por la legislación en vigor y será objeto de publicación en el «Boletín Oficial del País Vasco». El procedimiento de elaboración de la citada orden será el previsto para la elaboración de disposiciones de carácter general.

2. En el caso de ficheros de datos de carácter personal de otras administraciones, instituciones o corporaciones, el acuerdo o disposición por la que se cree, modifique o suprima deberá contener todas las menciones exigidas y será publicada en el «Boletín Oficial del País Vasco» o del territorio histórico, según sea el ámbito territorial al que se extienden sus funciones o competencias.

Artículo 5. *Recogida de datos de carácter personal.*

Las administraciones públicas y demás instituciones, corporaciones y entidades a que se refiere el artículo 2.1 de esta ley sólo podrán recoger datos de carácter personal para su tratamiento cuando sean adecuados, pertinentes y no excesivos para el ejercicio de las respectivas competencias que tienen atribuidas. Salvo precepto legal en sentido contrario, para la obtención de dichos datos no será preciso recabar el consentimiento de los afectados, pero sólo podrán utilizarse para las finalidades determinadas, explícitas y legítimas para las que se hubieran obtenido, sin perjuicio de su posible tratamiento posterior para fines históricos, estadísticos o científicos, de acuerdo con la legislación aplicable.

Artículo 6. *Información a los interesados.*

Los interesados a los que se soliciten datos de carácter personal serán previamente informados, de conformidad con la legislación sobre protección de dichos datos. No obstante, cuando los datos no hayan sido recabados del propio interesado y la información a éste resulte imposible o exija esfuerzos desproporcionados, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias, el director de la Agencia Vasca de Protección de Datos, de acuerdo con la susodicha legislación, podrá dispensar al responsable del fichero de la obligación de informar a los interesados.

Artículo 7. *Aprobación del contenido mínimo del documento de seguridad.*

En el ejercicio de sus potestades de autoorganización, los órganos de gobierno de las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1 de esta ley podrán aprobar, en aplicación de los preceptos relativos a la seguridad de los datos y para aplicar a todos o parte de los ficheros de los que son titulares sus respectivas administraciones, instituciones o corporaciones, el contenido mínimo del documento de seguridad que, en todo caso, deberán elaborar e implantar los responsables de fichero para garantizar la seguridad de los datos de carácter personal contenidos en los citados ficheros.

Artículo 8. *Procedimiento para el ejercicio de los derechos de los interesados.*

1. Los interesados podrán ejercitar los derechos de oposición, acceso, rectificación, cancelación y cualesquiera otros que les reconozca la ley. El contenido material de los mismos será el determinado en la ley.

2. Cada administración, institución o corporación regulará reglamentariamente el procedimiento para el ejercicio de los derechos señalados en el número anterior, en relación

con los ficheros de su titularidad a los que es de aplicación esta ley. No se exigirá contraprestación alguna por ello.

Artículo 9. *Reclamaciones ante la Agencia Vasca de Protección de Datos.*

1. Las actuaciones contrarias a lo dispuesto en esta ley pueden ser objeto de reclamación por los interesados ante la Agencia Vasca de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio del derecho de oposición, acceso, rectificación, cancelación o cualquier otro que le reconozca la legislación sobre protección de datos de carácter personal, podrá ponerlo en conocimiento de la Agencia Vasca de Protección de Datos, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que se debe dictar y notificar la resolución expresa de tutela de derechos es de seis meses, entendiéndose el silencio administrativo como desestimatorio de la tutela pedida.

4. Contra las resoluciones de la Agencia Vasca de Protección de Datos procederá recurso contencioso-administrativo. Podrá interponerse con carácter previo, potestativamente, recurso de reposición.

TÍTULO II

La Agencia Vasca de Protección de Datos

Artículo 10. *Creación y régimen jurídico.*

1. Se crea la Agencia Vasca de Protección de Datos como ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en esta ley y en su estatuto propio, que será aprobado por decreto del Gobierno Vasco a propuesta de la Vicepresidencia.

2. La Agencia Vasca de Protección de Datos sujetará su actividad a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuando ejerza potestades administrativas. En el resto de su actividad se someterá a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en esta ley y en las disposiciones de desarrollo de las mismas.

3. La Agencia Vasca de Protección de Datos estará sujeta al derecho público vigente en materia de adquisiciones patrimoniales y contratación. Sus bienes y derechos pertenecerán al patrimonio de la Comunidad Autónoma del País Vasco.

4. La representación y defensa en juicio de la Agencia Vasca de Protección de Datos estará a cargo de los servicios jurídicos de la Administración de la Comunidad Autónoma del País Vasco, conforme a lo dispuesto en sus normas reguladoras.

Artículo 11. *Personal.*

1. Los puestos de trabajo de la Agencia Vasca de Protección de Datos serán desempeñados por funcionarios de las administraciones públicas e instituciones a que se refiere el artículo 2.1 de esta ley y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal estará obligado a guardar secreto respecto a los datos de carácter personal que conozca en el desarrollo de su función.

2. El personal al servicio de la Agencia Vasca de Protección de Datos estará sometido a la normativa reguladora de la función pública en la Administración General de la Comunidad Autónoma. De conformidad con la misma, corresponde a la Agencia Vasca de Protección de Datos determinar el régimen de acceso a sus puestos de trabajo, los requisitos y las características de las pruebas de selección, así como la convocatoria, gestión y resolución de los procedimientos de provisión de puestos de trabajo y promoción profesional.

3. Los puestos de trabajo que comporten el ejercicio de potestades públicas estarán reservados a personal funcionario.

Artículo 12. *Recursos.*

La Agencia Vasca de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales de la Comunidad Autónoma.
b) Las subvenciones y aportaciones que se concedan a su favor.
c) Los ingresos, ordinarios y extraordinarios, derivados del ejercicio de sus actividades.
d) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.
e) Cualesquiera otros que legalmente puedan serle atribuidos.

Artículo 13. *Presupuesto.*

La Agencia Vasca de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno Vasco para que sea integrado, con la debida independencia, en los Presupuestos Generales de la Comunidad Autónoma, de acuerdo con la legislación reguladora del régimen presupuestario de la Comunidad Autónoma del País Vasco. Estará sometida a esta legislación en lo relativo al régimen de modificación, ejecución y liquidación de su presupuesto, atendiendo a estos efectos a la naturaleza de la entidad; al régimen de contabilidad pública y al control económico financiero y de gestión del Departamento de Hacienda y Administración Pública de la Administración de la Comunidad Autónoma, sin perjuicio de la fiscalización de sus actividades económico-financieras y contables por el Tribunal Vasco de Cuentas Públicas.

Artículo 14. *Órganos de gobierno.*

Son órganos de gobierno de la Agencia Vasca de Protección de Datos el director, el Consejo Consultivo y aquellos otros que se establezcan en su estatuto propio.

Artículo 15. *El director.*

1. El director de la Agencia Vasca de Protección de Datos dirige la agencia y ostenta su representación. Será nombrado por decreto del Gobierno Vasco, por un periodo de cuatro años.
2. Ejercerá sus funciones con plena independencia y objetividad, y no estará sujeto a instrucción alguna en el desempeño de aquellas. No obstante, el director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.
3. El director de la Agencia Vasca de Protección de Datos sólo cesará antes de la expiración de su periodo por alguna de las siguientes causas:

a) A petición propia.
b) Por separación, acordada por el Consejo de Gobierno, previa instrucción de expediente, en el que necesariamente será oído el Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

4. El director de la Agencia Vasca de Protección de Datos tendrá la consideración de alto cargo, quedará en la situación de servicios especiales si anteriormente estuviera desempeñando una función pública, y estará sometido al régimen de incompatibilidades de los altos cargos de la Administración de la Comunidad Autónoma.

Artículo 16. *El Consejo Consultivo.*

1. El director de la Agencia Vasca de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

a) Un representante del Parlamento Vasco, designado por éste.

b) Un representante de la Administración de la Comunidad Autónoma del País Vasco, designado por el Consejo de Gobierno.

c) Un representante de los territorios históricos, designado por éstos de común acuerdo.

d) Un representante de las entidades locales del ámbito territorial de la Comunidad Autónoma del País Vasco, designado por la asociación más representativa de las mismas en el citado ámbito territorial.

e) Dos expertos, uno en informática y otro en el ámbito de los derechos fundamentales, designados por la Universidad del País Vasco previa consulta a las corporaciones de derecho público de la Comunidad Autónoma del País Vasco.

2. El Consejo Consultivo aprobará sus propias normas de organización y funcionamiento, en las que se preverán las figuras de presidente y secretario, así como el sistema para su elección o designación.

Artículo 17. *Funciones.*

1. Son funciones de la Agencia Vasca de Protección de Datos, en relación con los ficheros a que se refiere el artículo 2.1 de esta ley y en el ámbito de las competencias de la Comunidad Autónoma del País Vasco:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) Emitir las autorizaciones previstas en las leyes y reglamentos.

c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la legislación vigente en materia de protección de datos.

d) Atender las peticiones y reclamaciones formuladas por los afectados.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f) Requerir a los responsables y a los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a la legislación en vigor y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros cuando no se ajuste a dicha legislación, salvo en la que se refiera a transferencias internacionales de datos.

g) Ejercer la potestad sancionadora y, en su caso, proponer la iniciación de procedimientos disciplinarios contra quienes estime responsables de las infracciones tipificadas en el artículo 22 de esta ley, así como adoptar las medidas cautelares que procedan, salvo en lo que se refiera a las transferencias internacionales de datos. Todo ello en los términos previstos en esta ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará anualmente una relación de dichos ficheros con la información adicional que el director de la Agencia Vasca de Protección de Datos determine.

k) Redactar una memoria anual y remitirla a la Vicepresidencia del Gobierno Vasco.

l) Velar por el cumplimiento de las disposiciones que la legislación sobre la función estadística pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 24.

m) Colaborar con la Agencia de Protección de Datos del Estado y entidades similares de otras comunidades autónomas en cuantas actividades sean necesarias para una mejor protección de la seguridad de los ficheros de datos de carácter personal y de los derechos de los ciudadanos en relación con los mismos.

n) Atender a las consultas que en materia de protección de datos de carácter personal le formulen las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1 de esta ley, así como otras personas físicas o jurídicas, en relación con los tratamientos de datos de carácter personal incluidos en el ámbito de aplicación de esta ley.

ñ) Cuantas otras le sean atribuidas por las leyes y reglamentos.

2. A los efectos de las funciones a que se refiere el número anterior, la Agencia Vasca de Protección de Datos tendrá la consideración de autoridad de control, y la ley le garantiza la plena independencia y objetividad en el ejercicio de su cometido.

Artículo 18. *Registro de Protección de Datos.*

1. Se crea el Registro de Protección de Datos, como órgano integrado en la Agencia Vasca de Protección de Datos en los términos que se establezcan en los estatutos de ésta.

2. Serán objeto de inscripción en el Registro de Protección de Datos:

a) Los ficheros a los que se refiere el artículo 2.1 de esta ley.

b) Las autorizaciones a las que se refiere la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

c) Los códigos tipo que afecten a los ficheros inscritos.

d) Los datos relativos a los ficheros inscritos que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. El Registro de Protección de Datos podrá denegar la inscripción solicitada cuando considere que la petición no se ajusta a derecho. En este caso, el director de la Agencia Vasca de Protección de Datos deberá requerir al solicitante para que efectúe las correcciones oportunas.

4. Reglamentariamente se regulará el procedimiento de inscripción de los ficheros a los que se refiere el artículo 2.1 de esta ley en el Registro de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes, y demás extremos pertinentes.

5. El Registro de Protección de Datos será de consulta pública y gratuita. Cualquier persona podrá conocer, recabando la información oportuna del citado registro, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento.

Artículo 19. *Potestad de inspección.*

1. La Agencia Vasca de Protección de Datos, como autoridad de control, podrá inspeccionar los ficheros a los que se refiere el artículo 2.1 de esta ley, recabando cuanta información precise para el cumplimiento de su cometido. A tal efecto, podrá solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de datos, accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el número anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos, y estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de sus funciones, incluso después de haber cesado en las mismas.

Artículo 20. *Requerimientos a los titulares de los ficheros.*

Cuando el director de la Agencia Vasca de Protección de Datos constate que el mantenimiento y uso de un determinado fichero incluido en el ámbito de aplicación de esta ley contraviene algún precepto de la misma o de las disposiciones que la desarrollen, podrá requerir a la administración pública, institución o corporación titular del fichero que adopte las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento. Si la administración requerida incumpliera el requerimiento formulado, el director de la Agencia Vasca de Protección de Datos, sin perjuicio de otras medidas que pueda adoptar de acuerdo con el artículo 17.f) de esta ley, podrá recurrir la resolución o la actitud omisiva adoptada por aquella administración, teniendo, a estos efectos, la condición de interesado.

TÍTULO III

Régimen sancionador

Artículo 21. *Responsables.*

Los responsables de los ficheros a los que se refiere el artículo 2.1 de esta ley y los encargados de los tratamientos de los mismos estarán sujetos al régimen de infracciones y sanciones establecido en esta ley.

Artículo 22. *Tipos de infracciones.*

1. Las infracciones se calificarán como leves, graves o muy graves.
2. Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento, cuando legalmente proceda.
b) No proporcionar la información que solicite la Agencia Vasca de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro de Protección de Datos, cuando no sea constitutivo de infracción grave.
d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información legalmente exigida.
e) Incumplir el deber de secreto legalmente establecido, salvo que constituya infracción grave.

3. Son infracciones graves:

a) Proceder a la creación de ficheros, o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general publicada en el «Boletín Oficial del País Vasco» o en el del territorio histórico correspondiente.
b) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigido.
c) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías legalmente establecidos o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.
d) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
e) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente proceda cuando resulten afectados los derechos de las personas amparadas por la legislación de protección de datos de carácter personal.
f) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales o a Hacienda pública, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.
g) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad.
h) No remitir a la Agencia Vasca de Protección de Datos las comunicaciones previstas en las leyes y reglamentos, así como no proporcionar a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquélla a tales efectos.
i) La obstrucción al ejercicio de la función inspectora.
j) No inscribir el fichero de datos de carácter personal en el Registro de Protección de Datos, cuando haya sido requerido para ello por el director de la Agencia Vasca de Protección de Datos.

k) Incumplir el deber de información legalmente establecido, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.
b) La comunicación o cesión de datos de carácter personal, fuera de los casos en que estén permitidas.
c) Recabar y tratar datos de carácter personal que revelen ideología, afiliación sindical, religión o creencias, cuando no medie consentimiento expreso del afectado.
d) Recabar y tratar datos referidos al origen racial, a la salud o a la vida sexual, cuando no lo disponga una ley o el afectado no haya consentido expresamente.
e) Crear ficheros con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual.
f) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el director de la Agencia Vasca de Protección de Datos o por los titulares del derecho de acceso.
g) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
h) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hace referencia la letra e) de este mismo apartado, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
i) No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
j) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

5. La tipificación de infracciones que contiene este artículo se entiende sin perjuicio de las tipificadas en la legislación estatal sobre protección de datos, en aquellos aspectos sobre los que la Comunidad Autónoma del País Vasco carece de competencia.

Artículo 23. *Tipos de sanciones.*

1. Las infracciones leves serán sancionadas con multa de 601,01 a 60.101,21 euros.
2. Las infracciones graves serán sancionadas con multa de 60.101,21 a 300.506,05 euros.
3. Las infracciones muy graves serán sancionadas con multa de 300.506,05 a 601.012,1 euros.
4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.
5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquélla en que se integra la considerada en el caso de que se trate.
6. En ningún caso podrá imponerse una sanción más grave que la fijada en la ley para la clase de infracción en la que se integre la que se pretenda sancionar.
7. El Gobierno Vasco actualizará periódicamente la cuantía de las sanciones, de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 24. *Infracciones cometidas por las administraciones públicas, instituciones y corporaciones de Derecho público.*

1. Cuando, instruido el correspondiente procedimiento, se llegue a la conclusión de que se ha cometido alguna o algunas de las infracciones a que se refiere el artículo anterior, en relación con los ficheros a que se refiere el artículo 2.1 de esta ley, el director de la Agencia Vasca de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados, si los hubiera, y la misma agota la vía administrativa.

2. El director de la Agencia Vasca de Protección de Datos podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán los establecidos en la legislación reguladora del régimen disciplinario de los funcionarios y personal al servicio de las administraciones públicas, instituciones y corporaciones a las que se refiere el artículo 2.1 de esta ley. A estos efectos, las infracciones tipificadas en esta ley completarán el régimen disciplinario que sea de aplicación.

3. En el supuesto de que haya que seguir un procedimiento sancionador, se estará a lo dispuesto en la Ley 2/1998, de 20 de febrero, de la Potestad Sancionadora de las Administraciones Públicas de la Comunidad Autónoma del País Vasco.

4. Se deberán comunicar a la Agencia Vasca de Protección de Datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los números anteriores.

5. El director de la Agencia Vasca de Protección de Datos comunicará al Ararteko las actuaciones que efectúe y las resoluciones que dicte al amparo de los números anteriores.

Artículo 25. *Inmovilización de ficheros.*

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el director de la Agencia Vasca de Protección de Datos podrá requerir a los responsables de ficheros de datos de carácter personal la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

Disposición adicional primera. *Comunicación de ficheros a la Agencia Vasca de Protección de Datos.*

Las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1) de esta ley comunicarán a la Agencia Vasca de Protección de Datos, en el plazo de tres meses a partir de la entrada en vigor de esta ley, los ficheros de datos de carácter personal señalados en aquel precepto que sean de su titularidad. Previamente deberán tener aprobada y publicada la disposición reguladora del correspondiente fichero.

Disposición adicional segunda. *Comunicación de datos del padrón.*

1. Las administraciones general y forales de la Comunidad Autónoma del País Vasco podrán solicitar al Euskal Estatistika-Erakundea/Instituto Vasco de Estadística, en los términos que se establecen en la disposición adicional segunda de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y artículo 17.3 de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población. Estos ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico-administrativas derivadas de las competencias respectivas de las administraciones públicas.

2. A los efectos de lo dispuesto en el párrafo anterior, se modifica el artículo 29 de la Ley 4/1986, de 28 de abril, de Estadística de la Comunidad Autónoma de Euskadi, en los siguientes términos: la redacción actual del citado precepto queda como número 1 del mismo, al que se añade un número 2 con el siguiente texto:

> «2. El Euskal Estatistika-Erakundea/Instituto Vasco de Estadística actuará también como depositario de copias de los padrones municipales de todos los municipios de la Comunidad Autónoma del País Vasco, a cuyos efectos éstos le deberán remitir copias de los citados registros administrativos en los términos que se establezcan reglamentariamente.»

Disposición adicional tercera. *Competencias del Ararteko y de la Agencia de Protección de Datos del Estado.*

Lo dispuesto en esta ley se entiende sin perjuicio de las competencias que tengan atribuidas el Ararteko y la Agencia de Protección de Datos del Estado.

Disposición final. *Desarrollo y aplicación.*

1. Se autoriza al Gobierno Vasco para el desarrollo y aplicación de lo dispuesto en esta ley.

2. Se autoriza al Departamento de Hacienda y Administración Pública para crear la sección presupuestaria correspondiente y para realizar, de acuerdo con la legislación reguladora del régimen presupuestario de la Comunidad Autónoma del País Vasco, las modificaciones presupuestarias precisas para la aplicación de lo dispuesto en esta ley.

§ 24

Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos

Comunidad Autónoma de Cataluña
«DOGC» núm. 5731, de 8 de octubre de 2010
«BOE» núm. 257, de 23 de octubre de 2010
Última modificación: 13 de marzo de 2015
Referencia: BOE-A-2010-16136

EL PRESIDENTE DE LA GENERALIDAD DE CATALUÑA

Sea notorio a todos los ciudadanos que el Parlamento de Cataluña ha aprobado y yo, en nombre del Rey y de acuerdo con lo que establece el artículo 65 del Estatuto de autonomía de Cataluña, promulgo la siguiente Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.

PREÁMBULO

La recogida y el tratamiento de información por parte de las entidades que forman el sector público, necesarios para el desarrollo de las funciones que les encomienda el ordenamiento jurídico, ha experimentado en los últimos años un considerable crecimiento, derivado no solo de la ampliación de la actividad del sector público, sino, fundamentalmente, del espectacular crecimiento de las posibilidades que ofrecen los medios tecnológicos para el tratamiento de la información. En este contexto y ante los riesgos que este fenómeno comporta, adquiere una relevancia creciente el derecho a la protección de datos, no únicamente para preservar el derecho a la intimidad, sino también, con carácter instrumental, para preservar los demás derechos de la persona reconocidos por la Constitución, el Estatuto de autonomía y el resto del ordenamiento jurídico.

El derecho a la protección de datos está reconocido por el Convenio 108, de 28 de enero de 1981, del Consejo de Europa, por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, así como por el artículo 18.4 de la Constitución española y el artículo 31 del Estatuto de autonomía. Regulado en el ámbito estatal por la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, el derecho a la protección de datos comporta no solo el poder jurídico de imponer a terceros el deber de abstenerse de cualquier intromisión en la esfera íntima de la persona, sino, más allá de eso, un poder de disposición sobre los datos personales que se traduce en el reconocimiento del derecho a que se requiera el consentimiento para el uso y la recogida de dichos datos personales, del derecho a ser informado, del derecho a acceder, rectificar, cancelar dichos datos y oponerse a su utilización en determinados supuestos, así como del derecho a que la recogida y el tratamiento sean realizados en condiciones que garanticen su seguridad.

La Agencia Catalana de Protección de Datos, autoridad independiente creada por la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, ha velado por la garantía del derecho a la protección de datos en el ámbito de las administraciones públicas de Cataluña mediante el asesoramiento, la difusión del derecho y el cumplimiento de las funciones de control establecidas por el ordenamiento jurídico.

La aprobación del Estatuto de autonomía de 2006 supuso el reconocimiento expreso, por vez primera en el ámbito estatutario, del derecho a la protección de datos y reforzó el papel de la autoridad de control en materia de protección de datos, ya que, por una parte, clarificó y amplió su ámbito de actuación y, por otra, reforzó su independencia al establecer su designación parlamentaria.

Junto con estas exigencias derivadas del Estatuto de autonomía y otras mejoras técnicas necesarias, es preciso también incorporar a la legislación vigente en Cataluña otras modificaciones, como la propia denominación de la autoridad, para evitar la confusión de su naturaleza con el de las entidades de carácter instrumental que bajo la denominación de agencias han aparecido últimamente en el ámbito administrativo.

CAPÍTULO I

Disposiciones generales

Artículo 1. *La Autoridad Catalana de Protección de Datos.*

La Autoridad Catalana de Protección de Datos es el organismo independiente que tiene por objeto garantizar, en el ámbito de las competencias de la Generalidad, los derechos a la protección de datos personales y de acceso a la información vinculada a ellos.

Artículo 2. *Naturaleza jurídica.*

1. La Autoridad Catalana de Protección de Datos es una institución de derecho público, con personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines, con plena autonomía orgánica y funcional, que actúa con objetividad y plena independencia de las administraciones públicas en el ejercicio de sus funciones.

2. La Autoridad Catalana de Protección de Datos se relaciona con el Gobierno mediante el departamento que se determine por reglamento.

Artículo 3. *Ámbito de actuación.*

El ámbito de actuación de la Autoridad Catalana de Protección de Datos comprende los ficheros y los tratamientos que llevan a cabo:

a) Las instituciones públicas.

b) La Administración de la Generalidad.

c) Los entes locales.

d) Las entidades autónomas, los consorcios y las demás entidades de derecho público vinculadas a la Administración de la Generalidad o a los entes locales, o que dependen de ellos.

e) Las entidades de derecho privado que cumplan, como mínimo, uno de los tres requisitos siguientes con relación a la Generalidad, a los entes locales o a los entes que dependen de ellos:

Primero.–Que su capital pertenezca mayoritariamente a dichos entes públicos.

Segundo.–Que sus ingresos presupuestarios provengan mayoritariamente de dichos entes públicos.

Tercero.–Que en sus órganos directivos los miembros designados por dichos entes públicos sean mayoría.

f) Las demás entidades de derecho privado que prestan servicios públicos mediante cualquier forma de gestión directa o indirecta, si se trata de ficheros y tratamientos vinculados a la prestación de dichos servicios.

g) Las universidades públicas y privadas que integran el sistema universitario catalán, y los entes que de ellas dependen.

h) Las personas físicas o jurídicas que cumplen funciones públicas con relación a materias que son competencia de la Generalidad o de los entes locales, si se trata de ficheros o tratamientos destinados al ejercicio de dichas funciones y el tratamiento se lleva a cabo en Cataluña.

i) Las corporaciones de derecho público que cumplen sus funciones exclusivamente en el ámbito territorial de Cataluña a los efectos de lo establecido por la presente ley.

Artículo 4. *Competencias.*

Para el cumplimiento de las funciones que la presente ley le asigna y dentro de su ámbito de actuación, corresponden a la Autoridad Catalana de Protección de Datos las competencias de registro, control, inspección, sanción y resolución, así como la aprobación de propuestas, recomendaciones e instrucciones.

Artículo 5. *Funciones.*

Las funciones de la Autoridad Catalana de Protección de Datos son:

a) Velar por el cumplimiento de la legislación vigente sobre protección de datos de carácter personal.

b) Resolver las reclamaciones de tutela formuladas por las personas afectadas respecto al ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

c) Promover, en el ámbito de sus competencias, la divulgación de los derechos de las personas con relación a la protección de datos y el acceso a la información, y la evaluación del impacto sobre la privacidad.

d) Velar por el cumplimiento de las disposiciones que la Ley 23/1998, de 30 de diciembre, de estadística de Cataluña establece respecto a la recogida de datos estadísticos y al secreto estadístico, y adoptar las medidas correspondientes para garantizar las condiciones de seguridad de los ficheros constituidos con finalidades exclusivamente estadísticas, sin perjuicio de las competencias atribuidas al Instituto de Estadística de Cataluña. A tales efectos, la Autoridad, en el ámbito de sus competencias, puede adoptar instrucciones y resoluciones dirigidas a los órganos administrativos y puede solicitar, si procede, la colaboración del Instituto de Estadística de Cataluña.

e) Dictar, sin perjuicio de las competencias de otros órganos e instituciones, las instrucciones y las recomendaciones en materia de protección de datos de carácter personal y de acceso a la información.

f) Requerir a los responsables del fichero o del tratamiento y a los encargados del tratamiento la adopción de las medidas necesarias para la adecuación del tratamiento de los datos personales objeto de investigación a la legislación vigente en materia de protección de datos de carácter personal y, en su caso, ordenar el cese de los tratamientos y la supresión de los ficheros.

g) Proporcionar información sobre los derechos de las personas en materia de tratamiento de datos personales.

h) Atender las peticiones de información, las quejas y las denuncias.

i) Decidir sobre las inscripciones de ficheros y el tratamiento de datos de carácter personal en el Registro de Protección de Datos de Cataluña, así como tener conocimiento de los demás ficheros en que, a pesar de estar exentos del deber de inscripción en el Registro, la legislación vigente establezca un deber de comunicación a la autoridad de protección de datos.

j) Ejercer la potestad de inspección.

k) Ejercer la potestad sancionadora sobre cualquier tipo de fichero o tratamiento sometido a la normativa de protección de datos, en el ámbito que establece el artículo 3.

l) Elaborar planes de auditoría.

m) Emitir informe, con carácter preceptivo, sobre los proyectos de disposiciones de carácter general de la Generalidad de creación, modificación o supresión de ficheros de datos de carácter personal, y sobre las disposiciones que afecten a la protección de datos de carácter personal.

n) Emitir informe, con carácter potestativo, sobre los proyectos de disposiciones de carácter general de los entes locales de creación, modificación o supresión de ficheros, y

sobre las disposiciones que tengan impacto en materia de protección de datos de carácter personal que los entes locales le sometan.

o) Responder a las consultas que formulen las entidades de su ámbito de actuación sobre la protección de datos de carácter personal al poder de las administraciones públicas y colaborar con estas entidades en la difusión de las obligaciones derivadas de la legislación reguladora de estas materias.

p) Otorgar las autorizaciones para la exención del deber de información en la recogida de datos, para el mantenimiento íntegro de determinados datos y las demás autorizaciones que establece la normativa vigente en materia de protección de datos.

q) Colaborar con la Agencia Española de Protección de Datos y con las demás agencias autonómicas, de acuerdo con lo establecido por la normativa reguladora de la agencia estatal.

r) Cumplir las demás funciones que le sean atribuidas de acuerdo con las leyes.

CAPÍTULO II

Organización

Artículo 6. *Órganos de gobierno.*

Los órganos de la Autoridad Catalana de Protección de Datos son:

a) El director o directora.

b) El Consejo Asesor de Protección de Datos.

Artículo 7. *El director o directora.*

1. El director o directora de la Autoridad Catalana de Protección de Datos dirige la institución y ejerce su representación.

2. El director o directora de la Autoridad Catalana de Protección de Datos, con sujeción al ordenamiento jurídico, con plena independencia y objetividad y sin sujeción a mandato imperativo alguno ni a instrucción de ninguna clase, ejerce las funciones que establece el artículo 8 y las que se establezcan por ley o reglamento.

3. El director o directora de la Autoridad Catalana de Protección de Datos es designado por el Pleno del Parlamento por mayoría de tres quintas partes, a propuesta del Consejo Asesor de Protección de Datos, de entre personas con condición política de catalanes, con pleno uso de sus derechos civiles y políticos y con experiencia en materia de protección de datos. Si no obtiene la mayoría requerida, debe someterse a una segunda votación, en la misma sesión del Pleno, en que requiere el voto favorable de la mayoría absoluta de los miembros de la cámara.

4. Los candidatos a director o directora de la Autoridad Catalana de Protección de Datos que proponga el Consejo Asesor de Protección de Datos deben comparecer ante la correspondiente comisión del Parlamento de Cataluña para que sus miembros puedan pedir las pertinentes aclaraciones y explicaciones sobre cualquier aspecto relacionado con su formación académica, trayectoria profesional o méritos alegados.

5. El director o directora de la Autoridad Catalana de Protección de Datos es elegido por un periodo de cinco años, renovable una sola vez.

6. El director o directora de la Autoridad Catalana de Protección de Datos cesa por las siguientes causas:

a) Por expiración del plazo del mandato.

b) A petición propia.

c) Por separación, acordada por el Pleno del Parlamento por mayoría de tres quintas partes, por incumplimiento grave de sus obligaciones, incompatibilidad, incapacidad sobrevenida para el ejercicio de sus funciones declarada por sentencia firme o condena firme por delito doloso.

7. El director o directora de la Autoridad Catalana de Protección de Datos tiene la consideración de alto cargo, asimilado al de secretario o secretaria general. El cargo, sin

perjuicio del régimen de incompatibilidades de los altos cargos al servicio de la Generalidad, es incompatible con:

a) El ejercicio de cualquier mandato representativo.

b) El ejercicio de funciones directivas o ejecutivas en partidos políticos, sindicatos o asociaciones empresariales, o el estar afiliado a ellos.

c) La pertenencia al Consejo de Garantías Estatutarias o al Tribunal Constitucional.

d) El ejercicio de cualquier cargo político o función administrativa en organismos internacionales, la Unión Europea, el Estado, las comunidades autónomas o las entidades locales.

e) El ejercicio de las carreras judicial, fiscal o militar.

f) El desarrollo de cualquier actividad profesional, mercantil, industrial o laboral.

Artículo 8. *Funciones del director o directora.*

1. Corresponde al director o directora de la Autoridad Catalana de Protección de Datos dictar las resoluciones y las instrucciones y aprobar las recomendaciones y los dictámenes que requiera el ejercicio de las funciones de la Autoridad, y en especial aprobar las instrucciones a que se refiere el artículo 15.

2. Corresponden al director o directora de la Autoridad Catalana de Protección de Datos, en el ámbito específico de las competencias de la Autoridad, las siguientes funciones:

a) Resolver motivadamente sobre la procedencia o improcedencia de las inscripciones que deban practicarse en el Registro de Protección de Datos de Cataluña.

b) Resolver motivadamente sobre la procedencia o improcedencia de la denegación del ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

c) Requerir a los responsables y a los encargados del tratamiento la adopción de las medidas necesarias para la adecuación del tratamiento de datos personales objeto de investigación a la legislación vigente y ordenar, si procede, el cese de los tratamientos y la cancelación de los ficheros.

d) Adoptar las medidas, resoluciones e instrucciones necesarias para garantizar las condiciones de seguridad de los ficheros constituidos con finalidades exclusivamente estadísticas.

e) Dictar las instrucciones y recomendaciones necesarias para adecuar los tratamientos de datos personales a los principios de la legislación vigente en materia de datos personales.

f) Emitir informe, con carácter preceptivo, de los anteproyectos de ley, de los proyectos de disposiciones normativas que elabore el Gobierno por delegación legislativa y de los proyectos de reglamentos o disposiciones de carácter general que afecten a la protección de datos de carácter personal.

g) Responder a las consultas que la Administración de la Generalidad, los entes locales y las universidades de Cataluña le formulen sobre la aplicación de la legislación de protección de datos de carácter personal.

h) Resolver sobre la adopción de medidas para corregir los efectos de las infracciones.

i) Proponer el inicio de actuaciones disciplinarias contra los responsables o los encargados del tratamiento, de acuerdo con lo establecido por la legislación vigente sobre régimen disciplinario de las administraciones públicas.

j) Resolver los expedientes sancionadores que sean de su competencia y poner en conocimiento de la Agencia Española de Protección de Datos las presuntas infracciones cuya sanción le corresponda.

k) Ordenar el cese del tratamiento, de la comunicación ilícita de datos o la inmovilización de los ficheros, cuando proceda.

l) Proporcionar información sobre los derechos de las personas en materia de tratamiento de datos personales.

m) Cumplir las funciones con relación a los planes de auditoría de la Autoridad a que se refiere el artículo 20.

n) Atender las peticiones que le formulen los ciudadanos.

o) Responder a las consultas que le formulen las administraciones.

p) Elaborar la memoria anual de las actuaciones y actividades de la Autoridad a que se refiere el artículo 13 y comparecer ante la comisión pertinente del Parlamento para informar de su contenido.

q) Cumplir cualquier otra que le sea encomendada por ley o reglamento.

3. Corresponden al director o directora de la Autoridad Catalana de Protección de Datos, en los ámbitos económico, de contratación y de recursos humanos de la Autoridad, las siguientes funciones:

a) Adjudicar y formalizar los contratos que requiera la gestión de la Autoridad y vigilar su cumplimiento y ejecución.

b) Aprobar los gastos y ordenar los pagos, dentro de los límites de los créditos del presupuesto de gastos de la Autoridad.

c) Elaborar el anteproyecto de presupuesto de la Autoridad y someterlo a la consideración del Consejo Asesor de Protección de Datos.

d) Aprobar la plantilla de personal de la Autoridad.

Artículo 9. *El Consejo Asesor de Protección de Datos.*

1. El Consejo Asesor de Protección de Datos es el órgano de asesoramiento y participación de la Autoridad Catalana de Protección de Datos y está constituido por los siguientes miembros:

a) El presidente o presidenta, que es nombrado por el Consejo de entre sus miembros, una vez efectuada la renovación ordinaria de los miembros designados por el Parlamento.

b) Tres personas designadas por el Parlamento, por mayoría de tres quintas partes. Si no obtienen la mayoría requerida, deben someterse a una segunda votación, en la misma sesión del Pleno, en que se requiere el voto favorable de la mayoría absoluta.

c) Tres personas en representación de la Administración de la Generalidad, designadas por el Gobierno.

d) Dos personas en representación de la Administración local de Cataluña, designadas por el Consejo de Gobiernos Locales.

e) Una persona experta en el ámbito de los derechos fundamentales, designada por el Consejo Interuniversitario de Cataluña.

f) Una persona experta en informática, designada por el Consejo Interuniversitario de Cataluña.

g) Una persona designada por el Instituto de Estudios Catalanes.

h) Una persona en representación de las organizaciones de consumidores y usuarios, designada por el Consejo de las Personas Consumidoras de Cataluña.

i) El director o directora del Instituto de Estadística de Cataluña.

j) Un funcionario o funcionaria de la Autoridad Catalana de Protección de Datos, que actúa de secretario o secretaria del Consejo.

2. La renovación de los miembros del Consejo Asesor de Protección de Datos se lleva a cabo cada cinco años de acuerdo con los estatutos de la Autoridad Catalana de Protección de Datos.

3. El director o directora de la Autoridad Catalana de Protección de Datos asiste a las reuniones del Consejo Asesor de Protección de Datos con voz y sin voto.

Artículo 10. *Funciones del Consejo Asesor de Protección de Datos.*

1. Las funciones del Consejo Asesor de Protección de Datos son:

a) Proponer al Parlamento la persona o personas candidatas a ocupar el puesto de director o directora de la Autoridad.

b) Emitir informe sobre los proyectos de instrucciones de la Autoridad que le sean sometidos.

c) Emitir informe sobre el anteproyecto de presupuesto anual de la Autoridad que el director o directora proponga.

d) Asesorar al director o directora de la Autoridad sobre cuantas cuestiones le sean sometidas.

e) Elaborar un informe preceptivo previo a la aprobación de la plantilla del personal de la Autoridad.

f) Elaborar un informe vinculante sobre el número máximo de trabajadores de la plantilla de personal eventual de la Autoridad.

g) Elaborar estudios y propuestas en materia de protección de datos de carácter personal y pedir al director o directora el establecimiento de criterios en la materia.

2. El Consejo Asesor de Protección de Datos ha de ser informado de:

a) La actividad de la Autoridad Catalana de Protección de Datos, por parte del director o directora y de forma periódica.

b) La memoria anual de la Autoridad.

c) Los criterios objetivos de los planes de auditoría a que se refiere el artículo 20.

3. El Consejo Asesor de Protección de Datos se rige por las normas que se establezcan por reglamento y, supletoriamente, por las disposiciones vigentes sobre funcionamiento de órganos colegiados de la Administración de la Generalidad.

Artículo 11. *El Registro de Protección de Datos de Cataluña.*

1. El Registro de Protección de Datos de Cataluña se integra en la Autoridad Catalana de Protección de Datos.

2. Son objeto de inscripción en el Registro de Protección de Datos de Cataluña:

a) Los ficheros de datos personales, de titularidad pública o privada, incluidos dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos.

b) Los códigos tipo formulados por las entidades incluidas dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos.

c) Las autorizaciones de tratamientos de datos de carácter personal previstas en la legislación vigente.

3. El Gobierno debe establecer por reglamento el procedimiento de inscripción de la creación, la modificación y la supresión de ficheros en el Registro de Protección de Datos de Cataluña, así como el contenido de los asientos registrales.

4. El Registro de Protección de Datos de Cataluña es de consulta pública y gratuita. Cualquier persona puede consultar, como mínimo, la información sobre la existencia de un determinado tratamiento de datos de carácter personal, las finalidades y la identidad de la persona responsable del tratamiento.

5. La Autoridad Catalana de Protección de Datos debe establecer los acuerdos de cooperación necesarios con la Agencia Española de Protección de Datos para integrar la información registral y mantenerla actualizada.

CAPÍTULO III

Relaciones con otros organismos e instituciones

Artículo 12. *Colaboración con otras instituciones.*

La Autoridad Catalana de Protección de Datos puede suscribir convenios de colaboración con el Síndic de Greuges, los síndicos locales, el Instituto de Estadística de Cataluña, las universidades y otras instituciones y organismos de defensa de los derechos de las personas.

Artículo 13. *Memoria anual.*

1. La Autoridad Catalana de Protección de Datos debe elaborar una memoria anual de sus actividades y de las conclusiones de los trabajos y expedientes que ha tramitado.

2. La Autoridad Catalana de Protección de Datos debe presentar la memoria anual en el Parlamento y dar cuenta de la misma en el marco de la comisión correspondiente, y remitirla también al Gobierno, al Síndic de Greuges y al director o directora de la Agencia Española de Protección de Datos.

Artículo 14. *Relaciones entre la Autoridad Catalana de Protección de Datos y el Síndic de Greuges.*

Las relaciones entre la Autoridad Catalana de Protección de Datos y el Síndic de Greuges son de colaboración en el ámbito de sus respectivas competencias.

CAPÍTULO IV

Ejercicio de competencias y funciones

Artículo 15. *Instrucciones.*

1. El director o directora de la Autoridad Catalana de Protección de Datos puede aprobar instrucciones para la adecuación de los ficheros y los tratamientos de datos a los principios y garantías que establece la legislación vigente en materia de protección de datos.
2. El proyecto de instrucción debe someterse a información pública y a informe del Consejo Asesor de Protección de Datos. Igualmente, puede ser sometido a informe de la Comisión Jurídica Asesora.
3. Las instrucciones a que se refiere el apartado 1 se publican en el «Diari Oficial de la Generalitat de Catalunya» y en la sede electrónica de la Autoridad Catalana de Protección de Datos.

Artículo 16. *Tutela de los derechos de acceso, rectificación, oposición y cancelación.*

1. Las personas interesadas a las que se deniegue, total o parcialmente, el ejercicio de los derechos de acceso, de rectificación, de cancelación o de oposición, o que puedan entender desestimada su solicitud por el hecho de no haber sido resuelta y remitida dentro del plazo establecido, pueden presentar una reclamación ante la Autoridad Catalana de Protección de Datos.
2. La Autoridad Catalana de Protección de Datos debe resolver expresamente sobre la procedencia o improcedencia de la reclamación a que se refiere el apartado 1 en el plazo de seis meses, previa audiencia de la persona responsable del fichero así como de las personas interesadas si el resultado del primer trámite de audiencia lo hace necesario. Transcurrido dicho plazo sin que la Autoridad notifique la resolución, se entiende que ha sido desestimada.
3. La resolución de estimación total o parcial de la tutela de un derecho ha de establecer el plazo en que este debe hacerse efectivo.
4. Si la solicitud de ejercicio del derecho ante la persona responsable del fichero es estimada, total o parcialmente, pero el derecho no se ha hecho efectivo en la forma y los plazos exigibles de acuerdo con la normativa aplicable, las personas interesadas pueden ponerlo en conocimiento de la Autoridad Catalana de Protección de Datos para que se lleven a cabo las correspondientes actuaciones sancionadoras.

Artículo 17. *Publicidad de los informes y resoluciones.*

1. La Autoridad Catalana de Protección de Datos está obligada a garantizar la confidencialidad de las consultas y reclamaciones de que tenga conocimiento, sin perjuicio del derecho de acceso a la información y documentación administrativas de las personas interesadas.
2. Los dictámenes, informes y resoluciones de la Autoridad Catalana de Protección de Datos deben hacerse públicos, una vez notificados a las personas interesadas, previa «anonimización» de los datos de carácter personal, sin perjuicio de lo establecido por el apartado 1.
3. De forma excepcional, puede optarse por no publicar las resoluciones sin interés doctrinal alguno o que, pese a la «anonimización», sea aconsejable por causas justificadas evitar su publicidad para impedir hacer reconocibles a las personas que lo solicitan.

Artículo 18. *Funciones de control.*

1. La actividad de control de la Autoridad Catalana de Protección de Datos se lleva a cabo mediante la potestad de inspección, los planes de auditoría, la aplicación del régimen sancionador, los requerimientos de adecuación a la legalidad y la potestad de inmovilización de ficheros.

2. Los hechos constatados por los funcionarios al servicio de la Autoridad Catalana de Protección de Datos al llevar a cabo su tarea de control e inspección, si sus actuaciones se formalizan en un documento público en que se observen los requisitos legales pertinentes, tienen valor probatorio, sin perjuicio de las pruebas en defensa de los respectivos derechos o intereses que puedan aportar los propios interesados.

Artículo 19. *Potestad de inspección.*

1. La Autoridad Catalana de Protección de Datos puede inspeccionar los ficheros y los tratamientos de datos personales a que se refiere la presente ley, a fin de obtener todas las informaciones necesarias para el ejercicio de sus funciones. A tal fin, la Autoridad puede solicitar la presentación o la remisión de documentos y de datos o examinarlos en el lugar donde estén depositados, así como inspeccionar los equipos físicos y lógicos utilizados, para lo cual puede acceder a los locales donde estén instalados.

2. Los funcionarios que ejercen la función inspectora a que se refiere el apartado 1 tienen la consideración de autoridad pública en el desarrollo de su actividad y quedan obligados a mantener el secreto sobre las informaciones que conozcan en el ejercicio de las funciones inspectoras, incluso después de haber cesado en las mismas.

3. En el ejercicio de las funciones de inspección los funcionarios pueden ser auxiliados por personal no funcionario, si así lo decide el director o directora de la Autoridad, en función de los conocimientos de orden técnico que puedan ser necesarios para auditar sistemas de información durante las tareas de investigación. El personal no funcionario que participa en la actividad inspectora debe hacerlo siguiendo las instrucciones y bajo la supervisión del personal funcionario inspector, y tiene las mismas obligaciones que este, especialmente en cuanto al deber de secreto.

4. Las entidades comprendidas dentro del ámbito de aplicación de la presente ley tienen la obligación de auxiliar, con carácter preferente y urgente, a la Autoridad Catalana de Protección de Datos en sus investigaciones, si esta lo solicita.

Artículo 20. *Planes de auditoría.*

1. Los planes de auditoría de la Autoridad Catalana de Protección de Datos constituyen un sistema de control preventivo para:

a) Verificar el cumplimiento de la normativa en materia de protección de datos de carácter personal.

b) Recomendar o requerir a los responsables de los ficheros y de los tratamientos de datos de carácter personal la adopción de las medidas correctoras adecuadas.

2. Corresponde al director o directora de la Autoridad Catalana de Protección de Datos:

a) Decidir el contenido de cada plan de auditoría y concretar los aspectos y tratamientos que deben ser analizados.

b) Seleccionar las entidades que deben ser objeto de los planes de auditoría mediante criterios objetivos que han de ser públicos.

3. Las entidades a que se refiere la letra b del apartado 2 deben colaborar con la persona responsable de la auditoría facilitando la realización de las verificaciones oportunas y aportando la información y documentación necesarias.

4. Las conclusiones de los planes de auditoría sobre el grado general de cumplimiento y las recomendaciones generales pertinentes deben difundirse públicamente.

5. Si durante el proceso de ejecución de un plan de auditoría la entidad afectada es objeto, previa denuncia, de la incoación de un expediente sancionador por parte de la Autoridad Catalana de Protección de Datos como consecuencia de la comisión de una posible infracción por algún aspecto coincidente o directamente relacionado con el contenido

del plan de auditoría que se está llevando a cabo, la entidad debe ser excluida del plan de auditoría y debe continuarse la tramitación del procedimiento sancionador.

6. Los requerimientos a que se refiere la letra b del apartado 1 deben establecer un plazo adecuado para la adopción de las medidas correctoras necesarias por parte de las entidades afectadas. Transcurrido dicho plazo sin que la entidad afectada informe a la Autoridad Catalana de Protección de Datos sobre las medidas adoptadas, o si estas son insuficientes o inadecuadas, la Autoridad puede iniciar las actuaciones inspectoras oportunas para incoar, si procede, un procedimiento sancionador.

Artículo 21. *Régimen sancionador.*

1. Los responsables de los ficheros y de los tratamientos de datos personales incluidos dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos y los encargados de los correspondientes tratamientos quedan sujetos al régimen sancionador establecido por la legislación estatal de protección de datos de carácter personal. Las referencias a la Agencia Española de Protección de Datos o a sus órganos, en cuanto al régimen de infracciones, deben entenderse hechas a la Autoridad Catalana de Protección de Datos o a sus órganos, en lo concerniente a su ámbito competencial.

2. En el caso de infracciones cometidas con relación a ficheros de titularidad pública, el director o directora de la Autoridad Catalana de Protección de Datos debe dictar una resolución que declare la infracción y establezca las medidas a adoptar para corregir sus efectos. Además, puede proponer, si procede, la iniciación de actuaciones disciplinarias de acuerdo con lo establecido por la legislación vigente sobre el régimen disciplinario del personal al servicio de las administraciones públicas. Dicha resolución debe notificarse a la persona responsable del fichero o del tratamiento, a la encargada del tratamiento, si procede, al órgano del que dependan y a las personas afectadas, si las hay.

3. En el caso de infracciones cometidas con relación a ficheros de titularidad privada, la resolución que declare la infracción debe imponer las sanciones previstas por la legislación de protección de datos y las medidas a adoptar para corregir los efectos de la infracción.

4. El director o directora de la Autoridad Catalana de Protección de Datos debe informar al síndic o síndica de greuges de las actuaciones que haga a consecuencia de una solicitud del mismo y debe comunicarle las resoluciones sancionadoras que dicte con relación a dichas actuaciones.

Artículo 22. *Procedimiento sancionador.*

1. El Gobierno debe establecer por decreto el procedimiento para la determinación de las infracciones y la imposición de sanciones.

2. La denuncia que inicia un procedimiento sancionador debe formalizarse mediante escrito razonado y estar debidamente firmada.

3. La persona denunciante debe identificarse en el momento de hacer la denuncia a que se refiere el apartado 2. Sin embargo, puede solicitar de forma razonada que su identidad no sea revelada, previa ponderación de los intereses en conflicto por la Autoridad Catalana de Protección de Datos, cuando haya motivos fundamentados y legítimos relativos a una situación personal concreta que así lo justifique.

4. La persona denunciante tiene derecho a que le sean comunicadas las actuaciones que se deriven de su denuncia, sin perjuicio de los derechos que puedan corresponderle si también es persona interesada.

Artículo 23. *Medidas provisionales.*

En el momento de la incoación o durante la tramitación del procedimiento sancionador, el director o directora de la Autoridad Catalana de Protección de Datos puede adoptar, de forma motivada, las medidas provisionales que considere necesarias para asegurar la eficacia de la resolución que finalmente pueda recaer y para conseguir la protección provisional del derecho a la protección de datos de las personas afectadas. Con carácter previo, la Autoridad debe dar audiencia a las entidades afectadas, excepto si concurren circunstancias de urgencia que puedan hacer perder la finalidad de la medida. La resolución que adopte la medida es susceptible de los recursos procedentes.

Artículo 24. *Cumplimiento de la resolución del procedimiento sancionador.*

1. En las infracciones declaradas respecto a ficheros de titularidad pública, las personas o entidades que hayan sido declaradas responsables de la infracción deben comunicar a la Autoridad Catalana de Protección de Datos, en el plazo que establece la resolución, la adopción de las medidas y actuaciones a que se refiere el apartado 2 del artículo 25.

2. En las sanciones impuestas por infracciones cometidas respecto a ficheros de titularidad privada, el cumplimiento de la sanción debe llevarse a cabo en el plazo establecido por la legislación vigente. Dentro de este plazo, la entidad sancionada puede solicitar, de forma razonada, el fraccionamiento del pago. El director o directora de la Autoridad Catalana de Protección de Datos debe resolver la solicitud, de acuerdo con lo establecido por la normativa reguladora de la recaudación de los ingresos públicos.

3. Las personas o entidades sancionadas a quienes se haya impuesto alguna medida correctora de acuerdo con lo establecido por el artículo 25 deben comunicar a la Autoridad Catalana de Protección de Datos, en el plazo que establece la resolución, las medidas adoptadas.

Artículo 25. *Requerimientos de adecuación y potestad de inmovilización.*

1. En los supuestos, constitutivos de infracción muy grave, de utilización o de comunicación ilícita de datos personales en que se atente gravemente contra los derechos fundamentales y las libertades públicas de los ciudadanos o se impida su ejercicio, el director o directora de la Autoridad Catalana de Protección de Datos puede exigir a los responsables de los ficheros de datos personales el cese de la utilización o comunicación ilícita de datos personales.

2. Si el requerimiento a que se refiere el apartado 1 no es atendido, el director o directora de la Autoridad Catalana de Protección de Datos puede, mediante resolución motivada, inmovilizar los ficheros de datos personales, con la única finalidad de restaurar los derechos de las personas afectadas. En este supuesto, la inmovilización queda sin efecto de no acordar la Autoridad, en el plazo de quince días, la incoación de un procedimiento sancionador y ratificarse la medida.

CAPÍTULO V

Régimen jurídico, de personal, económico y de contratación

Artículo 26. *Régimen jurídico.*

1. La Autoridad Catalana de Protección de Datos, en el ejercicio de sus funciones, actúa de conformidad con lo dispuesto por la presente ley, sus disposiciones de desarrollo y la legislación reguladora del régimen jurídico de las administraciones públicas y el procedimiento administrativo aplicable a la Administración de la Generalidad.

2. Las resoluciones del director o directora de la Autoridad Catalana de Protección de Datos agotan la vía administrativa y son susceptibles de recurso contencioso-administrativo, sin perjuicio de los recursos administrativos que procedan.

Artículo 27. *Régimen de personal.*

1. La Autoridad Catalana de Protección de Datos, en el ejercicio de su potestad de autoorganización y de acuerdo con los créditos consignados en los presupuestos de la Generalidad, aprueba la relación de puestos de trabajo de los órganos y servicios que la integran y que han de ser ocupados por personal funcionario, laboral o eventual, e informa de ello al Parlamento.

2. Al personal al servicio de la Autoridad Catalana de Protección de Datos se le aplica a todos los efectos la normativa que regula el estatuto del personal al servicio de la Administración de la Generalidad en cuanto al régimen y la normativa de ordenación de la ocupación pública.

3. Los puestos de trabajo que comportan el ejercicio de potestades públicas se reservan a personal funcionario.

4. Los puestos de trabajo considerados de confianza o de asesoramiento especial no reservado a personal funcionario y que figuran con este carácter en la correspondiente relación de puestos de trabajo son desempeñados por personal eventual, cuyo número máximo fija el Consejo Asesor de Protección de Datos.

5. La Autoridad Catalana de Protección de Datos ejerce la potestad disciplinaria respecto al personal al servicio de la institución.

6. El personal al servicio de la Autoridad Catalana de Protección de Datos tiene el deber de secreto sobre las informaciones que conozca en el ejercicio de sus funciones, incluso después de haber cesado en su ejercicio.

Artículo 28. *Régimen económico y de contratación.*

1. Para el cumplimiento de sus finalidades, la Autoridad Catalana de Protección de Datos cuenta con los siguientes bienes y recursos económicos:

a) Las asignaciones anuales de los presupuestos de la Generalidad.

b) Los bienes y derechos que constituyen su patrimonio, así como los productos y rentas de los mismos.

c) El producto de las sanciones que imponga en el ejercicio de sus competencias.

d) El producto de las tasas y demás ingresos públicos devengados por su actividad.

e) Cualquier otro recurso económico que legalmente se le pueda atribuir.

2. **(Derogado).**

3. La Autoridad Catalana de Protección de Datos debe elaborar su propuesta de anteproyecto de presupuesto de ingresos y de gastos de acuerdo con las normas que dicte el departamento competente en materia de economía y finanzas para elaborar los presupuestos de la Generalidad, y debe remitirlo al departamento mediante el que se relaciona con el Gobierno para que este, sobre la base de esta propuesta, formule el anteproyecto y tramite su inclusión en el proyecto de ley de presupuestos de la Generalidad.

4. La Autoridad Catalana de Protección de Datos está sometida al control financiero de la Intervención General de la Generalidad y al régimen de contabilidad pública.

5. El régimen jurídico de contratación de la Autoridad Catalana de Protección de Datos es el establecido por la legislación sobre contratos del sector público.

6. El régimen patrimonial de la Autoridad Catalana de Protección de Datos es el establecido por la normativa que regula el patrimonio de la Administración de la Generalidad.

Disposición transitoria primera. *Sucesión de la Agencia Catalana de Protección de Datos.*

1. La Autoridad Catalana de Protección de Datos se subroga en la posición jurídica de la Agencia Catalana de Protección de Datos en cuanto a los bienes, derechos y obligaciones de cualquier tipo de que fuera titular la Agencia.

2. Las referencias hechas en el ordenamiento jurídico a la Agencia Catalana de Protección de Datos deben entenderse hechas a la Autoridad Catalana de Protección de Datos.

Disposición transitoria segunda. *Procedimiento sancionador.*

Mientras el Gobierno no apruebe el decreto que regula el procedimiento sancionador en materia de protección de datos, continúa siendo aplicable el procedimiento establecido por el Decreto 278/1993, de 9 de noviembre, sobre procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad.

Disposición transitoria tercera. *Vigencia del Estatuto de la Agencia Catalana de Protección de Datos.*

Mientras no entren en vigor los estatutos de la Autoridad Catalana de Protección de Datos, sigue siendo de aplicación, en todo lo que no se oponga a la presente ley, el Estatuto de la Agencia Catalana de Protección de Datos, aprobado por el Decreto 48/2003, de 20 de febrero.

Disposición derogatoria.

Queda derogada la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos.

Disposición final primera. *Estatutos de la Autoridad.*

En el plazo de seis meses a contar desde la entrada en vigor de la presente ley, el Gobierno debe aprobar los estatutos de la Autoridad Catalana de Protección de Datos.

Disposición final segunda. *Desarrollo de los procedimientos.*

Se habilita al Gobierno para la regulación de los procedimientos necesarios para el ejercicio de las funciones atribuidas a la Autoridad Catalana de Protección de Datos, sin perjuicio de la competencia de la Autoridad para concretar mediante instrucción aquellos aspectos en que sea necesario.

Disposición final tercera. *Creación, modificación y supresión de ficheros.*

1. Los consejeros de la Generalidad, dentro del ámbito de sus respectivas competencias, quedan habilitados para crear, modificar y suprimir, mediante orden, los ficheros de sus departamentos o de los entes públicos vinculados a ellos o que dependan de los mismos y los ficheros de los consorcios en que la representación de la Administración de la Generalidad en los órganos de gobierno sea mayoritaria.

2. Las entidades de derecho público dotadas de especial independencia o autonomía quedan habilitadas para ejercer la competencia de crear, modificar y suprimir ficheros.

§ 25

Ley 7/2017, de 2 de noviembre, por la que se incorpora al ordenamiento jurídico español la Directiva 2013/11/UE, del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 268, de 4 de noviembre de 2017
Última modificación: sin modificaciones
Referencia: BOE-A-2017-12659

[. . .]

TÍTULO II

Obligaciones de las entidades de resolución alternativa acreditadas

[. . .]

Artículo 36. *Garantías de confidencialidad y de protección de datos de carácter personal.*

1. Las entidades acreditadas garantizarán que los procedimientos de resolución alternativa de litigios que gestionen sean confidenciales.

A estos efectos, y entre otras actuaciones, velarán para que tanto las personas encargadas de la decisión del litigio, sujetas al secreto profesional, como las partes en litigio, no revelen la información que hubieran podido obtener con ocasión del procedimiento.

2. Las entidades acreditadas adoptarán las medidas necesarias para asegurar que el tratamiento de los datos personales cumpla con lo establecido en la normativa vigente en materia de protección de datos de carácter personal.

Esta obligación se extenderá al tratamiento de datos llevado a cabo con ocasión de la tramitación de los procedimientos de resolución alternativa como consecuencia de las cesiones que se efectúen en el marco de la cooperación e intercambio de información de las entidades acreditadas o sus redes y en el intercambio de información con autoridades y administraciones públicas.

3. La infracción del deber de confidencialidad por las entidades acreditadas o por las personas encargadas de la decisión del litigio generará la responsabilidad prevista en el ordenamiento jurídico.

Artículo 37. *Actualización de información.*

Las entidades acreditadas trasladarán a la autoridad competente que corresponda, dentro del plazo de 15 días laborables, cualquier modificación que afecte a los datos comunicados por las mismas, así como a los requisitos, obligaciones y garantías exigidas en esta ley.

[. . .]

§ 26

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 236, de 2 de octubre de 2015
Última modificación: 4 de julio de 2018
Referencia: BOE-A-2015-10566

[. . .]

TÍTULO PRELIMINAR

Disposiciones generales, principios de actuación y funcionamiento del sector público

CAPÍTULO I

Disposiciones generales

[. . .]

Artículo 3. *Principios generales.*

1. Las Administraciones Públicas sirven con objetividad los intereses generales y actúan de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Constitución, a la Ley y al Derecho.

Deberán respetar en su actuación y relaciones los siguientes principios:

a) Servicio efectivo a los ciudadanos.
b) Simplicidad, claridad y proximidad a los ciudadanos.
c) Participación, objetividad y transparencia de la actuación administrativa.
d) Racionalización y agilidad de los procedimientos administrativos y de las actividades materiales de gestión.
e) Buena fe, confianza legítima y lealtad institucional.
f) Responsabilidad por la gestión pública.
g) Planificación y dirección por objetivos y control de la gestión y evaluación de los resultados de las políticas públicas.
h) Eficacia en el cumplimiento de los objetivos fijados.
i) Economía, suficiencia y adecuación estricta de los medios a los fines institucionales.

j) Eficiencia en la asignación y utilización de los recursos públicos.
k) Cooperación, colaboración y coordinación entre las Administraciones Públicas.

2. Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

3. Bajo la dirección del Gobierno de la Nación, de los órganos de gobierno de las Comunidades Autónomas y de los correspondientes de las Entidades Locales, la actuación de la Administración Pública respectiva se desarrolla para alcanzar los objetivos que establecen las leyes y el resto del ordenamiento jurídico.

4. Cada una de las Administraciones Públicas del artículo 2 actúa para el cumplimiento de sus fines con personalidad jurídica única.

[. . .]

CAPÍTULO V

Funcionamiento electrónico del sector público

Artículo 38. *La sede electrónica.*

1. La sede electrónica es aquella dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a una o varios organismos públicos o entidades de Derecho Público en el ejercicio de sus competencias.

2. El establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.

3. Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de transparencia, publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. En todo caso deberá garantizarse la identificación del órgano titular de la sede, así como los medios disponibles para la formulación de sugerencias y quejas.

4. Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.

5. La publicación en las sedes electrónicas de informaciones, servicios y transacciones respetará los principios de accesibilidad y uso de acuerdo con las normas establecidas al respecto, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

6. Las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, certificados reconocidos o cualificados de autenticación de sitio web o medio equivalente.

Artículo 39. *Portal de internet.*

Se entiende por portal de internet el punto de acceso electrónico cuya titularidad corresponda a una Administración Pública, organismo público o entidad de Derecho Público que permite el acceso a través de internet a la información publicada y, en su caso, a la sede electrónica correspondiente.

Artículo 40. *Sistemas de identificación de las Administraciones Públicas.*

1. Las Administraciones Públicas podrán identificarse mediante el uso de un sello electrónico basado en un certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica. Estos certificados electrónicos incluirán el número de identificación fiscal y la denominación correspondiente, así como, en su caso, la identidad de la persona titular en el caso de los sellos electrónicos de órganos

administrativos. La relación de sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

2. Se entenderá identificada la Administración Pública respecto de la información que se publique como propia en su portal de internet.

Artículo 41. *Actuación administrativa automatizada.*

1. Se entiende por actuación administrativa automatizada, cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público.

2. En caso de actuación administrativa automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.

Artículo 42. *Sistemas de firma para la actuación administrativa automatizada.*

En el ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

a) Sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, basado en certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación vinculado a la Administración Pública, órgano, organismo público o entidad de Derecho Público, en los términos y condiciones establecidos, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Artículo 43. *Firma electrónica del personal al servicio de las Administraciones Públicas.*

1. Sin perjuicio de lo previsto en los artículos 38, 41 y 42, la actuación de una Administración Pública, órgano, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante firma electrónica del titular del órgano o empleado público.

2. Cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios. Por razones de seguridad pública los sistemas de firma electrónica podrán referirse sólo el número de identificación profesional del empleado público.

Artículo 44. *Intercambio electrónico de datos en entornos cerrados de comunicación.*

1. Los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones Públicas, órganos, organismos públicos y entidades de derecho público, serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en este artículo.

2. Cuando los participantes en las comunicaciones pertenezcan a una misma Administración Pública, ésta determinará las condiciones y garantías por las que se regirá que, al menos, comprenderá la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

3. Cuando los participantes pertenezcan a distintas Administraciones, las condiciones y garantías citadas en el apartado anterior se establecerán mediante convenio suscrito entre aquellas.

4. En todo caso deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

Artículo 45. *Aseguramiento e interoperabilidad de la firma electrónica.*

1. Las Administraciones Públicas podrán determinar los trámites e informes que incluyan firma electrónica reconocida o cualificada y avanzada basada en certificados electrónicos reconocidos o cualificados de firma electrónica.

2. Con el fin de favorecer la interoperabilidad y posibilitar la verificación automática de la firma electrónica de los documentos electrónicos, cuando una Administración utilice sistemas de firma electrónica distintos de aquellos basados en certificado electrónico reconocido o cualificado, para remitir o poner a disposición de otros órganos, organismos públicos, entidades de Derecho Público o Administraciones la documentación firmada electrónicamente, podrá superponer un sello electrónico basado en un certificado electrónico reconocido o cualificado.

Artículo 46. *Archivo electrónico de documentos.*

1. Todos los documentos utilizados en las actuaciones administrativas se almacenarán por medios electrónicos, salvo cuando no sea posible.

2. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, el cumplimiento de las garantías previstas en la legislación de protección de datos, así como la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones Públicas que así lo requieran, de acuerdo con las especificaciones sobre el ciclo de vida de los servicios y sistemas utilizados.

[. . .]

§ 27

Acuerdo de 23 de julio de 2015, del Pleno del Tribunal Constitucional, por el que se regula la exclusión de los datos de identidad personal en la publicación de las resoluciones jurisdiccionales

Tribunal Constitucional
«BOE» núm. 178, de 27 de julio de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-8372

El Pleno del Tribunal Constitucional, en ejercicio de la competencia definida en el artículo 2.2, en relación con el artículo 10.1.m), de la Ley Orgánica 2/1979, de 3 de octubre, ha adoptado el siguiente acuerdo:

Artículo 1.

El Tribunal Constitucional en sus resoluciones jurisdiccionales preservará de oficio el anonimato de los menores y personas que requieran un especial deber de tutela, de las víctimas de delitos de cuya difusión se deriven especiales perjuicios y de las personas que no estén constituidas en parte en el proceso constitucional.

Artículo 2.

El Tribunal, en los demás casos, podrá excepcionar, de oficio o a instancia de parte, la exigencia constitucional de publicidad de sus resoluciones (artículo 164 CE), en lo relativo a los datos de identidad y situación personal de las partes intervinientes en el proceso.

A tal fin, si una parte estimase necesario que en un asunto sometido al conocimiento del Tribunal no se divulgue públicamente su identidad o situación personal, deberá solicitarlo en el momento de formular la demanda o en el de su personación, exponiendo los motivos de su petición.

El Tribunal accederá a la petición cuando, a partir de la ponderación de circunstancias debidamente acreditadas concurrentes en el caso, la estime justificada por resultar prevalente el derecho a la intimidad u otros intereses constitucionales.

Artículo 3.

En los casos en que proceda preservar el anonimato de las personas concernidas por la publicación de las resoluciones del Tribunal Constitucional, se sustituirá su identidad por las iniciales correspondientes y se omitirán los demás datos que permitan su identificación.

Disposición transitoria.

Las disposiciones de este acuerdo serán aplicables a los procesos iniciados antes de su entrada en vigor.

Disposición final.

El presente acuerdo entrará en vigor el día de su publicación en el «Boletín oficial del Estado».

§ 28

Ley 23/2015, de 21 de julio, Ordenadora del Sistema de Inspección de Trabajo y Seguridad Social. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 174, de 22 de julio de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-8168

[. . .]

TÍTULO II

Funcionamiento del Sistema

CAPÍTULO I

De las funciones de la Inspección de Trabajo y Seguridad Social

[. . .]

Artículo 16. *Auxilio y colaboración con la Inspección de Trabajo y Seguridad Social.*

1. Las autoridades, cualquiera que sea su naturaleza, los titulares de los órganos de la Administración General del Estado, de las Administraciones de las Comunidades Autónomas y de las Entidades Locales; los organismos autónomos y las entidades públicas empresariales; las cámaras y corporaciones, colegios y asociaciones profesionales; las demás entidades públicas, y quienes, en general, ejerzan funciones públicas, estarán obligados a suministrar a la Inspección de Trabajo y Seguridad Social cuantos datos, informes y antecedentes que tengan trascendencia en el ámbito de sus competencias, así como a prestarle la colaboración que le sea solicitada para el ejercicio de la función inspectora.

2. El Consejo General del Notariado suministrará a la Inspección de Trabajo y Seguridad Social, de forma telemática, la información contenida en el índice único informatizado regulado en el artículo 17 de la Ley del Notariado de 28 de mayo de 1862, que tenga trascendencia en el ejercicio de la función inspectora.

3. La Administración Tributaria cederá sus datos y antecedentes a la Inspección de Trabajo y Seguridad Social en los términos establecidos en el artículo 95.1.c) de la Ley 58/2003, de 17 de diciembre, General Tributaria. Asimismo, las entidades gestoras y colaboradoras y los servicios comunes de la Seguridad Social prestarán su colaboración a la Inspección de Trabajo y Seguridad Social, facilitándole, cuando le sean solicitadas, las

informaciones, antecedentes y datos con relevancia en el ejercicio de la función inspectora, incluso los de carácter personal objeto de tratamiento automatizado, sin necesidad de consentimiento del afectado. La Administración Tributaria y la Inspección de Trabajo y Seguridad Social establecerán programas de mutua correspondencia y de coordinación para el cumplimiento de sus fines.

4. Los órganos de la Administración General del Estado y los de las Comunidades Autónomas colaborarán con la Inspección de Trabajo y Seguridad Social y le prestarán el apoyo y el asesoramiento pericial y técnico necesario.

5. Las mutualidades de previsión social deberán colaborar y suministrar a la Inspección de Trabajo y Seguridad Social los datos e informes que resulten necesarios para el adecuado desarrollo de la actividad de la Inspección, en lo relativo a su condición de entidad alternativa al Régimen Especial de la Seguridad Social de los Trabajadores por Cuenta Propia o Autónomos.

6. Las obligaciones de auxilio y colaboración establecidas en los apartados anteriores sólo tendrán las limitaciones legalmente establecidas referentes a la intimidad de la persona, al secreto de la correspondencia, o de las informaciones suministradas a las Administraciones Públicas con finalidad exclusivamente estadística.

7. Las Fuerzas y Cuerpos de Seguridad competentes estarán obligadas a prestar apoyo, auxilio y colaboración a la Inspección de Trabajo y Seguridad Social en el desempeño de sus funciones, a través de los mandos designados a tal efecto por la autoridad correspondiente.

8. Mediante convenios u otros instrumentos se establecerán las formas de colaboración con la Inspección de Trabajo y Seguridad Social por parte de otros órganos de la Administración General del Estado o de otras Administraciones Públicas para los supuestos en que, como consecuencia de su actuación, tengan conocimiento de hechos presuntamente constitutivos de trabajo no declarado y empleo irregular.

Los hechos comprobados directamente por los funcionarios que ostenten la condición de Autoridad o de agentes de ella, contenidos en comunicaciones que se formulen en ejecución de lo establecido en los convenios o instrumentos indicados en el párrafo anterior, tras su valoración y calificación por la Inspección de Trabajo y Seguridad Social, podrán ser aducidos como prueba en los procedimientos iniciados por esta y serán tenidos por ciertos, salvo prueba en contrario de los interesados.

9. Los Juzgados y Tribunales facilitarán a la Inspección de Trabajo y Seguridad Social, de oficio o a petición de la misma, los datos de trascendencia para la función inspectora que se desprendan de las actuaciones en que conozcan y que no resulten afectados por el secreto sumarial.

10. La colaboración de las Autoridades de los Estados Miembros de la Unión Europea con competencias equivalentes a las de la Inspección de Trabajo y Seguridad Social se regirá por la normativa de la Unión Europea o por los instrumentos o acuerdos bilaterales o multilaterales de los que sea parte el Estado Español.

Los hechos comprobados por dichas autoridades en el ámbito de la cooperación administrativa internacional que sean facilitados a las autoridades españolas podrán ser aducidos como prueba por la Inspección de Trabajo y Seguridad Social en los procedimientos iniciados por esta y serán tenidos por ciertos, salvo prueba en contrario de los interesados.

11. La obtención de datos de carácter personal no recabados del interesado por los funcionarios de la Inspección en el ejercicio de sus competencias, no requerirá la información expresa e inequívoca a los interesados prevista en el artículo 5.4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[. . .]

Artículo 18. *De la colaboración con los funcionarios de la Inspección de Trabajo y Seguridad Social.*

1. Los empresarios, los trabajadores y los representantes de ambos, así como los demás sujetos responsables del cumplimiento de las normas del orden social, están obligados cuando sean requeridos:

a) A atender debidamente a los inspectores de Trabajo y Seguridad Social y a los Subinspectores Laborales.

b) A acreditar su identidad y la de quienes se encuentren en los centros de trabajo.

c) A colaborar con ellos con ocasión de visitas u otras actuaciones inspectoras.

d) A declarar ante el funcionario actuante sobre cuestiones que afecten a las comprobaciones inspectoras, así como a facilitarles la información y documentación necesarias para el desarrollo de sus funciones. Quienes representen a los sujetos inspeccionados deberán acreditar documentalmente tal condición si la actuación se produjese fuera del domicilio o centro de trabajo visitado.

2. Toda persona natural o jurídica estará obligada a proporcionar a la Inspección de Trabajo y Seguridad Social toda clase de datos, antecedentes o información con trascendencia en los cometidos inspectores, siempre que se deduzcan de sus relaciones económicas, profesionales, empresariales o financieras con terceros sujetos a la acción inspectora, cuando a ello sea requerida en forma. Tal obligación alcanza a las entidades colaboradoras de los órganos de recaudación de la Seguridad Social y a las depositarias de dinero en efectivo o de fondos en cuanto a la identificación de pagos realizados con cargo a las cuentas que pueda tener en dicha entidad la persona que se señale en el correspondiente requerimiento, sin que puedan ampararse en el secreto bancario. La obligación de los profesionales de facilitar información no alcanza a aquellos datos confidenciales a que hubieran accedido por su prestación de servicios de asesoramiento y defensa o con ocasión de prestaciones o atenciones sanitarias, salvo conformidad previa y expresa de los interesados. El incumplimiento de estos requerimientos se considerará como infracción por obstrucción conforme al texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, aprobado por el Real Decreto Legislativo 5/2000, de 4 de agosto. Reglamentariamente se determinará la forma y requisitos aplicables a los referidos requerimientos.

3. La colaboración con la Inspección de Trabajo y Seguridad Social se llevará a efecto, preferentemente, por medios electrónicos, conforme a lo dispuesto en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

4. De conformidad con lo previsto en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre, la transmisión a la Inspección de aquellos datos personales que sean necesarios para el ejercicio de la función inspectora, en virtud de su deber de colaboración, no estará sujeta a la necesidad de consentimiento del interesado.

Los datos que hubieran sido transmitidos únicamente se emplearán para ejercicio de las competencias atribuidas por esta ley a la Inspección de Trabajo y Seguridad Social.

CAPÍTULO II

De las actuaciones de la Inspección de Trabajo y Seguridad Social

[. . .]

Artículo 24. *Información del Sistema de Inspección de Trabajo y Seguridad Social.*

1. Conforme al principio de concepción única e integral del Sistema de Inspección de Trabajo y Seguridad Social, deberá garantizarse en el tratamiento de la información de dicho Sistema la unidad e integración de la información, la interoperabilidad, la interconexión y el acceso a la misma a las distintas Administraciones Públicas en función de las materias objeto de su competencia, en los términos establecidos en esta ley y su normativa de desarrollo.

En consecuencia, el personal del Sistema de Inspección de Trabajo y Seguridad Social, podrá acceder a la información necesaria para el ejercicio de las funciones inspectoras, de los registros y bases de datos disponibles, de acuerdo con lo dispuesto en el artículo 16 y en los términos que se establezcan.

2. El tratamiento de la información del Sistema debe realizarse a partir de una base de datos unitaria e integrada, que mantenga la homogeneidad de los datos y consolide, en el

conjunto del Estado, la información aportada por los servicios de la Inspección de Trabajo y Seguridad Social, así como la que se derive de sus actuaciones.

3. El tratamiento de los datos de carácter personal incorporados a la base de datos del Sistema se encuentra sujeto a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.

No obstante, no será necesario el consentimiento de los interesados para la inclusión de sus datos en la base de datos del Sistema ni para el acceso a los mismos o su comunicación a terceros por parte de las Administraciones Públicas competentes.

4. Serán de aplicación al sistema de información las medidas de seguridad de nivel alto establecidas en la normativa de protección de datos de carácter personal.

[. . .]

§ 29

Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 77, de 31 de marzo de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-3444

[. . .]

TÍTULO III

Órganos de vigilancia y control de los altos cargos de la Administración General del Estado

[. . .]

Artículo 21. *Registros.*

1. Los Registros electrónicos de Actividades y de Bienes y Derechos Patrimoniales de Altos Cargos se alojarán en un sistema de gestión documental que garantice la inalterabilidad y permanencia de sus datos, así como la alta seguridad en el acceso y uso de éstos.

2. El Registro electrónico de Actividades tendrá carácter público, rigiéndose por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, en la Ley 19/2013, de 9 de diciembre, en esta ley y en las normas de desarrollo de las leyes citadas.

3. El Registro electrónico de Bienes y Derechos Patrimoniales tendrá carácter reservado y solo podrán tener acceso al mismo además del propio interesado, los siguientes órganos:

a) El Congreso de los Diputados y el Senado, de acuerdo con lo que establezcan los reglamentos de las Cámaras, así como las comisiones parlamentarias de investigación que se constituyan.

b) Los órganos judiciales para la instrucción o resolución de procesos que requieran el conocimiento de los datos que obran en el Registro, de conformidad con lo dispuesto en las leyes procesales.

c) El Ministerio Fiscal cuando realice actuaciones de investigación en el ejercicio de sus funciones que requieran el conocimiento de los datos obrantes en el Registro.

4. Los órganos mencionados en el apartado anterior adoptarán las medidas necesarias para mantener el carácter reservado de la información contenida en el Registro electrónico de Bienes y Derechos Patrimoniales, sin perjuicio de la aplicación de las normas reguladoras de los procedimientos en cuya tramitación se hubiera solicitado la información.

5. El contenido de las declaraciones de bienes y derechos patrimoniales de los miembros del Gobierno y de los Secretarios de Estado y demás Altos Cargos se publicarán en el «Boletín Oficial del Estado», en los términos previstos reglamentariamente. En relación con los bienes patrimoniales, se publicará una declaración comprensiva de la situación patrimonial de estos Altos Cargos, omitiéndose aquellos datos referentes a su localización y salvaguardando la privacidad y seguridad de sus titulares.

[. . .]

§ 30

Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 156, de 27 de junio de 2014
Última modificación: 24 de noviembre de 2018
Referencia: BOE-A-2014-6726

[. . .]

TÍTULO I

De las entidades de crédito

CAPÍTULO I

Disposiciones generales

[. . .]

Artículo 5. *Protección del cliente de entidades de crédito.*

1. El Ministro de Economía y Competitividad, con el fin de proteger los legítimos intereses de los clientes de servicios o productos bancarios, distintos de los de inversión, prestados por las entidades de crédito, podrá dictar disposiciones relativas a:

a) La información precontractual que debe facilitarse a los clientes, la información y contenido de los contratos y las comunicaciones posteriores que permitan el seguimiento de los mismos, de modo que reflejen de forma explícita y con la máxima claridad los derechos y obligaciones de las partes, los riesgos derivados del servicio o producto para el cliente y las demás circunstancias necesarias para garantizar la transparencia de las condiciones más relevantes de los servicios o productos y permitir al cliente evaluar si estos se ajustan a sus necesidades y a su situación financiera. A tal efecto, los contratos de estos servicios o productos siempre se formalizarán por escrito o en formato electrónico o en otro soporte duradero y el Ministro de Economía y Competitividad podrá, en particular, fijar las cláusulas que los contratos referentes a servicios o productos bancarios típicos habrán de tratar o prever de forma expresa.

b) La transparencia de las condiciones básicas de comercialización o contratación de los servicios o productos bancarios que ofrecen las entidades de crédito y, en su caso, el deber

y la forma en que deben comunicar tales condiciones a su clientela o al Banco de España. Se podrán establecer, asimismo, condiciones básicas de los servicios o productos bancarios de debido cumplimiento para las entidades de crédito. En particular, solo podrán percibirse comisiones o repercutirse gastos por servicios solicitados en firme o aceptados expresamente por un cliente y siempre que respondan a servicios efectivamente prestados o gastos habidos que puedan acreditarse.

c) Los principios y criterios a los que debe sujetarse la actividad publicitaria de los servicios o productos bancarios, y las modalidades de control administrativo sobre la misma, con la finalidad de que ésta resulte clara, suficiente, objetiva y no engañosa.

d) Las especialidades de la contratación de servicios o productos bancarios de forma electrónica o por otras vías de comunicación a distancia y la información que, al objeto de lo previsto en este artículo, debe figurar en las páginas electrónicas de las entidades de crédito.

e) El ámbito de aplicación de las normas dictadas al amparo de este artículo a cualesquiera contratos u operaciones de la naturaleza prevista en dichas normas, aun cuando la entidad que intervenga no tenga la condición de entidad de crédito.

2. En particular, en la comercialización de préstamos o créditos, el Ministro de Economía y Competitividad podrá dictar normas que favorezcan:

a) La adecuada atención a los ingresos de los clientes en relación con los compromisos que adquieran al recibir un préstamo.

b) La adecuada e independiente valoración de las garantías inmobiliarias que aseguren los préstamos de forma que se contemplen mecanismos que eviten las influencias indebidas de la propia entidad o de sus filiales en la valoración.

c) La consideración de diferentes escenarios de evolución de los tipos en los préstamos a interés variable, las posibilidades de cobertura frente a tales variaciones y todo ello teniendo además en cuenta el uso o no de índices oficiales de referencia.

d) La obtención y documentación apropiada de datos relevantes del solicitante.

e) La información precontractual y asistencia apropiadas para el cliente.

f) El respeto de las normas de protección de datos.

Sin perjuicio de la libertad contractual, el Ministerio de Economía y Competitividad podrá efectuar, por sí o a través del Banco de España, la publicación regular, con carácter oficial, de determinados índices o tipos de interés de referencia que puedan ser aplicados por las entidades de crédito a los préstamos a interés variable, especialmente en el caso de créditos o préstamos hipotecarios.

3. Las disposiciones que en el ejercicio de sus competencias puedan dictar las Comunidades Autónomas sobre las materias contempladas en este artículo no podrán establecer un nivel de protección inferior al dispensado en las normas que apruebe el Ministro de Economía y Competitividad. Asimismo, podrán establecerse con carácter básico modelos normalizados de información que no podrán ser modificados por la normativa autonómica, en aras de la adecuada transparencia y homogeneidad de la información suministrada a los clientes de servicios o productos bancarios.

4. Las normas dictadas al amparo de lo previsto en este artículo serán consideradas normativa de ordenación y disciplina y su supervisión corresponderá al Banco de España.

[. . .]

TÍTULO III

Supervisión

CAPÍTULO I

Función supervisora

Artículo 50. *Función supervisora del Banco de España.*

1. El Banco de España es la autoridad responsable de la supervisión de las entidades de crédito y de las demás entidades previstas en el artículo 56, para garantizar el cumplimiento de la normativa de ordenación y disciplina. Para el ejercicio de esta función podrá desarrollar las actuaciones y ejercer las facultades previstas en esta Ley y cualesquiera otras que le atribuya el ordenamiento jurídico.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio de las competencias que el ordenamiento jurídico atribuya a otras instituciones u órganos administrativos.

2. En el ejercicio de su función supervisora y, en particular, para la elección de los distintos instrumentos de supervisión y sanción, el Banco de España podrá:

a) Recabar de las entidades y personas sujetas a su función supervisora, y a terceros a los que dichas entidades hayan subcontratado actividades o funciones operativas, la información necesaria para comprobar el cumplimiento de la normativa de ordenación y disciplina.

Con el fin de que el Banco de España pueda obtener dichas informaciones, o confirmar su veracidad, las entidades y personas mencionadas quedan obligadas a poner a disposición del Banco de España cuantos libros, registros y documentos considere precisos, incluidos los programas informáticos, ficheros y bases de datos, sea cuál sea su soporte físico o virtual.

A tales efectos, el acceso a las informaciones y datos requeridos por el Banco de España se encuentra amparado por el artículo 11.2.a) de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

b) Requerir y comunicar a las entidades sujetas a su función supervisora, por medios electrónicos, las informaciones y medidas recogidas en la normativa de ordenación y disciplina. Las entidades referidas tendrán obligación de habilitar, en el plazo que se fije para ello, los medios técnicos requeridos por el Banco de España para la eficacia de sus sistemas de comunicación electrónica, en los términos que éste adopte al efecto.

c) Llevar a cabo todas las investigaciones necesarias en relación con cualquier entidad o persona de las contempladas en la letra a), cuando sea necesario para desempeñar su función supervisora. A estos efectos, podrá:

1.º Exigir la presentación de documentos.

2.º Examinar los libros y registros y obtener copias o extractos de los mismos.

3.º Solicitar y obtener explicaciones escritas o verbales de cualquier otra persona diferente de las previstas en la letra a) a fin de recabar información relacionada con el objeto de una investigación.

d) Realizar cuantas inspecciones sean necesarias en los establecimientos profesionales de las personas jurídicas contempladas en la letra a), y en cualquier otra entidad incluida en la supervisión consolidada.

3. Asimismo, en el ejercicio de su función supervisora, el Banco de España deberá:

a) Valorar, en la elección de las medidas que se vayan a adoptar, criterios como la gravedad de los hechos detectados, la eficacia de la propia función supervisora en términos de la subsanación de los incumplimientos detectados o el comportamiento previo de la entidad.

b) Tomar en consideración la posible incidencia de sus decisiones en la estabilidad del sistema financiero de los demás Estados miembros de la Unión Europea afectados,

particularmente en situaciones de urgencia, basándose en la información disponible en el momento de que se trate.

c) Tener en cuenta la convergencia de instrumentos y prácticas de supervisión en el ámbito de la Unión Europea.

4. En los términos previstos por el artículo 4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los órganos y organismos de cualquier Administración Pública, sin perjuicio del deber de secreto que les ampare conforme a la legislación vigente quedan sujetos al deber de colaborar con el Banco de España y están obligados a proporcionar, a requerimiento de éste, los datos e informaciones de que dispongan y puedan resultar necesarios para el ejercicio por parte de éste de la función supervisora.

[. . .]

CAPÍTULO VI

Obligaciones de información y publicación

[. . .]

Artículo 83. *Deber de reserva de información.*

1. Las entidades y demás personas sujetas a la normativa de ordenación y disciplina de las entidades de crédito están obligadas a guardar reserva de las informaciones relativas a los saldos, posiciones, transacciones y demás operaciones de sus clientes sin que las mismas puedan ser comunicadas a terceros u objeto de divulgación.

2. Se exceptúan de este deber las informaciones respecto de las cuales el cliente o las leyes permitan su comunicación o divulgación a terceros o que, en su caso, les sean requeridas o hayan de remitir a las respectivas autoridades de supervisión o en el marco del cumplimiento de las obligaciones establecidas en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y la financiación del terrorismo. En este caso, la cesión de la información deberá ajustarse a lo dispuesto por el propio cliente o por las leyes.

3. Quedan asimismo exceptuadas del deber de reserva los intercambios de información entre entidades de crédito pertenecientes a un mismo grupo consolidable.

4. El incumplimiento de lo dispuesto en el presente artículo será considerado infracción grave y se sancionará en los términos y con arreglo al procedimiento previsto en el Título IV.

5. Lo previsto en este artículo se aplicará sin perjuicio de lo establecido en la normativa de protección de datos de carácter personal.

[. . .]

Artículo 115. *Publicidad de las sanciones.*

1. La imposición de las sanciones, con excepción de la de amonestación privada, se hará constar en los registros administrativos de entidades de crédito y altos cargos que correspondan.

2. Las sanciones de suspensión, separación y separación con inhabilitación, una vez sean ejecutivas, se harán constar, además, en el Registro Mercantil y, en su caso, en el Registro de Cooperativas.

3. El nombramiento de miembros del órgano de administración o de administradores provisionales a que se refiere el artículo 106, se hará constar también en los registros correspondientes.

4. Una vez que las sanciones impuestas a la entidad de crédito o a quienes ejerzan cargos de administración o dirección en la misma sean ejecutivas se comunicarán en la siguiente Junta o Asamblea General que se celebre.

5. Las sanciones y amonestaciones por infracciones muy graves y graves serán publicadas en el "Boletín Oficial del Estado" una vez que sean firmes en la vía administrativa. La publicación deberá incluir, por lo menos, información sobre el tipo y la naturaleza de la infracción y la identidad de las personas responsables de la misma.

6. En relación con lo previsto en el apartado anterior, excepcionalmente, el Banco de España podrá, o bien retrasar la publicación hasta el momento en que dejen de existir los motivos que justifiquen tal retraso, o bien publicar la sanción impuesta de forma anónima, cuando a su criterio se produzca alguna de las circunstancias siguientes:

a) Cuando la sanción se imponga a una persona física y, tras una evaluación previa, la publicación de los datos personales resulte ser desproporcionada.

b) Cuando la publicación pudiera poner en peligro la estabilidad de los mercados financieros o una investigación penal en curso.

c) Cuando la publicación pudiera causar un daño desproporcionado a las entidades o personas físicas implicadas, en la medida en que se pueda determinar el daño.

7. Las sanciones y amonestaciones por infracciones muy graves y graves deberán asimismo ser publicadas en la página web del Banco de España, en un plazo máximo de 15 días hábiles desde que la sanción o amonestación sea firme en vía administrativa, con el contenido de la información a la que se hace referencia en el apartado 5, pudiendo adoptarse las medidas contempladas en el apartado 6 en los supuestos en él previstos.

Cuando se interponga recurso en vía judicial contra la decisión de imponer una sanción o medida, el Banco de España también publicará de inmediato en su sitio web oficial esa información, así como toda información posterior relativa al resultado de ese recurso. Además, también se publicará toda decisión que anule o condone una decisión previa de imponer una sanción o medida.

El Banco de España mantendrá publicada toda la información a que se refieren los apartados anteriores en su sitio web oficial durante cinco años, como mínimo, tras su publicación.

[. . .]

§ 31

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 114, de 10 de mayo de 2014
Última modificación: 4 de julio de 2018
Referencia: BOE-A-2014-4950

[. . .]

TÍTULO III

Obligaciones de servicio público y derechos y obligaciones de carácter público en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas

[. . .]

CAPÍTULO III

Secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas

Artículo 39. *Secreto de las comunicaciones.*

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

2. Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la

interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, éste podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

4. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad o identidades del sujeto objeto de la medida de la interceptación.

Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica.

c) Servicios básicos utilizados.

d) Servicios suplementarios utilizados.

e) Dirección de la comunicación.

f) Indicación de respuesta.

g) Causa de finalización.

h) Marcas temporales.

i) Información de localización.

j) Información intercambiada a través del canal de control o señalización.

6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) Identificación de la persona física o jurídica.

b) Domicilio en el que el proveedor realiza las notificaciones.

Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:

c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).

d) Número de identificación del terminal.

e) Número de cuenta asignada por el proveedor de servicios Internet.

f) Dirección de correo electrónico.

7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.

8. Los sujetos obligados deberán facilitar al agente facultado, de entre los datos previstos en los apartados 5, 6 y 7 de este artículo, sólo aquéllos que estén incluidos en la orden de interceptación legal.

9. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de identidad de extranjero o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.

10. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que se establezcan por el Ministerio de Industria, Energía y Turismo.

11. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.

Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.

Artículo 40. *Interceptación de las comunicaciones electrónicas por los servicios técnicos.*

1. Con pleno respeto al derecho al secreto de las comunicaciones y a la exigencia, conforme a lo establecido en la Ley de Enjuiciamiento Criminal, de autorización judicial para la interceptación de contenidos, cuando para la realización de las tareas de control para la eficaz utilización del dominio público radioeléctrico o para la localización de interferencias perjudiciales sea necesaria la utilización de equipos, infraestructuras e instalaciones técnicas de interceptación de señales no dirigidas al público en general, será de aplicación lo siguiente:

a) La Administración de las telecomunicaciones deberá diseñar y establecer sus sistemas técnicos de interceptación de señales en forma tal que se reduzca al mínimo el riesgo de afectar a los contenidos de las comunicaciones.

b) Cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los soportes en los que éstos aparezcan deberán ser custodiados hasta la finalización, en su caso, del expediente sancionador que hubiera lugar o, en otro caso, destruidos inmediatamente. En ninguna circunstancia podrán ser objeto de divulgación.

2. Las mismas reglas se aplicarán para la vigilancia del adecuado empleo de las redes y la correcta prestación de los servicios de comunicaciones electrónicas.

3. Lo establecido en este artículo se entiende sin perjuicio de las facultades que a la Administración atribuye el artículo 60.

Artículo 41. *Protección de los datos de carácter personal.*

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar la protección de los datos de carácter personal. Dichas medidas incluirán, como mínimo:

a) La garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la Ley.

b) La protección de los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos.

c) La garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.

La Agencia Española de Protección de Datos, en el ejercicio de su competencia de garantía de la seguridad en el tratamiento de datos de carácter personal, podrá examinar las medidas adoptadas por los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público y podrá formular recomendaciones sobre las mejores prácticas con respecto al nivel de seguridad que debería conseguirse con estas medidas.

2. En caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar.

3. En caso de violación de los datos personales, el operador de servicios de comunicaciones electrónicas disponibles al público notificará sin dilaciones indebidas dicha violación a la Agencia Española de Protección de Datos. Si la violación de los datos pudiera afectar negativamente a la intimidad o a los datos personales de un abonado o particular, el operador notificará también la violación al abonado o particular sin dilaciones indebidas.

La notificación de una violación de los datos personales a un abonado o particular afectado no será necesaria si el proveedor ha probado a satisfacción de la Agencia Española de Protección de Datos que ha aplicado las medidas de protección tecnológica convenientes y que estas medidas se han aplicado a los datos afectados por la violación de seguridad. Unas medidas de protección de estas características podrían ser aquellas que convierten los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos.

Sin perjuicio de la obligación del proveedor de informar a los abonados o particulares afectados, si el proveedor no ha notificado ya al abonado o al particular la violación de los datos personales, la Agencia Española de Protección de Datos podrá exigirle que lo haga, una vez evaluados los posibles efectos adversos de la violación.

En la notificación al abonado o al particular se describirá al menos la naturaleza de la violación de los datos personales y los puntos de contacto donde puede obtenerse más información y se recomendarán medidas para atenuar los posibles efectos adversos de dicha violación. En la notificación a la Agencia Española de Protección de Datos se describirán además las consecuencias de la violación y las medidas propuestas o adoptadas por el proveedor respecto a la violación de los datos personales.

Los operadores deberán llevar un inventario de las violaciones de los datos personales, incluidos los hechos relacionados con tales infracciones, sus efectos y las medidas adoptadas al respecto, que resulte suficiente para permitir a la Agencia Española de Protección de Datos verificar el cumplimiento de las obligaciones de notificación reguladas en este apartado. Mediante real decreto podrá establecerse el formato y contenido del inventario.

A los efectos establecidos en este artículo, se entenderá como violación de los datos personales la violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público.

La Agencia Española de Protección de Datos podrá adoptar directrices y, en caso necesario, dictar instrucciones sobre las circunstancias en que se requiere que el proveedor notifique la violación de los datos personales, sobre el formato que debe adoptar dicha notificación y sobre la manera de llevarla a cabo, con pleno respeto a las disposiciones que en su caso sean adoptadas en esta materia por la Comisión Europea.

4. Lo dispuesto en el presente artículo será sin perjuicio de la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

Artículo 42. *Conservación y cesión de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.*

La conservación y cesión de los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación a los agentes facultados a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales se rige por lo establecido en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Artículo 43. *Cifrado en las redes y servicios de comunicaciones electrónicas.*

1. Cualquier tipo de información que se transmita por redes de comunicaciones electrónicas podrá ser protegida mediante procedimientos de cifrado.

2. El cifrado es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de facilitar a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, así como la obligación de facilitar sin coste alguno los aparatos de cifra a efectos de su control de acuerdo con la normativa vigente.

Artículo 44. *Integridad y seguridad de las redes y de los servicios de comunicaciones electrónicas.*

1. Los operadores de redes y de servicios de comunicaciones electrónicas disponibles al público, gestionarán adecuadamente los riesgos de seguridad que puedan afectar a sus redes y servicios a fin de garantizar un adecuado nivel de seguridad y evitar o reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y en las redes interconectadas.

2. Asimismo, los operadores de redes públicas de comunicaciones electrónicas garantizarán la integridad de las mismas a fin de asegurar la continuidad en la prestación de los servicios que utilizan dichas redes.

3. Los operadores que exploten redes o presten servicios de comunicaciones electrónicas disponibles al público notificarán al Ministerio de Industria, Energía y Turismo las violaciones de la seguridad o pérdidas de integridad que hayan tenido un impacto significativo en la explotación de las redes o los servicios.

Cuando proceda, el Ministerio informará a las autoridades nacionales competentes de otros Estados miembros y a la Agencia Europea de Seguridad en las Redes y la Información (ENISA). Asimismo, podrá informar al público o exigir a las empresas que lo hagan, en caso de estimar que la divulgación de la violación reviste interés público. Una vez al año, el Ministerio presentará a la Comisión y a la ENISA un informe resumido sobre las notificaciones recibidas y las medidas adoptadas de conformidad con este apartado.

Del mismo modo, el Ministerio comunicará a la Secretaría de Estado de Seguridad del Ministerio del Interior aquellos incidentes que afectando a los operadores estratégicos nacionales sean de interés para la mejora de la protección de infraestructuras críticas, en el marco de la Ley 8/2011, de 28 de abril, reguladora de las mismas. También el Ministerio comunicará a la Comisión Nacional de los Mercados y la Competencia las violaciones de la seguridad o pérdidas de integridad a que se refiere este apartado que afecten o puedan afectar a las obligaciones específicas impuestas por dicha Comisión en los mercados de referencia.

4. El Ministerio de Industria, Energía y Turismo establecerá los mecanismos para supervisar el cumplimiento de las obligaciones anteriores y, en su caso, dictará las instrucciones correspondientes, que serán vinculantes para los operadores, incluidas las relativas a las fechas límite de aplicación, para que adopten determinadas medidas relativas a la integridad y seguridad de redes y servicios de comunicaciones electrónicas. Entre ellas, podrá imponer:

a) La obligación de facilitar la información necesaria para evaluar la seguridad y la integridad de sus servicios y redes, incluidos los documentos sobre las políticas de seguridad.

b) La obligación de someterse a una auditoría de seguridad realizada por un organismo independiente o por una autoridad competente, y de poner el resultado a disposición del Ministerio de Industria, Energía y Turismo. El coste de la auditoría será sufragado por el operador.

5. En particular, los operadores garantizarán la mayor disponibilidad posible de los servicios telefónicos disponibles al público a través de las redes públicas de comunicaciones en caso de fallo catastrófico de la red o en casos de fuerza mayor, y adoptarán todas las medidas necesarias para garantizar el acceso sin interrupciones a los servicios de emergencia.

6. El presente artículo se entiende sin perjuicio de lo establecido en el apartado 4 del artículo 4 de la presente Ley.

[. . .]

§ 32

Ley 5/2014, de 4 de abril, de Seguridad Privada. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 83, de 5 de abril de 2014
Última modificación: sin modificaciones
Referencia: BOE-A-2014-3649

[. . .]

TÍTULO I

Coordinación

[. . .]

Artículo 15. *Acceso a la información por las Fuerzas y Cuerpos de Seguridad.*

1. Se autorizan las cesiones de datos que se consideren necesarias para contribuir a la salvaguarda de la seguridad ciudadana, así como el acceso por parte de las Fuerzas y Cuerpos de Seguridad a los sistemas instalados por las empresas de seguridad privada que permitan la comprobación de las informaciones en tiempo real cuando ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

2. El tratamiento de datos de carácter personal, así como los ficheros, automatizados o no, creados para el cumplimiento de esta ley se someterán a lo dispuesto en la normativa de protección de datos de carácter personal.

3. La comunicación de buena fe de información a las Fuerzas y Cuerpos de Seguridad por las entidades y el personal de seguridad privada no constituirá vulneración de las restricciones sobre divulgación de información impuestas por vía contractual o por cualquier disposición legal, reglamentaria o administrativa, cuando ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

[. . .]

TÍTULO IV

Servicios y medidas de seguridad

[. . .]

CAPÍTULO II

Servicios de las empresas de seguridad privada

[. . .]

Artículo 42. *Servicios de videovigilancia.*

1. Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas.

Cuando la finalidad de estos servicios sea prevenir infracciones y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados, serán prestados necesariamente por vigilantes de seguridad o, en su caso, por guardas rurales.

No tendrán la consideración de servicio de videovigilancia la utilización de cámaras o videocámaras cuyo objeto principal sea la comprobación del estado de instalaciones o bienes, el control de accesos a aparcamientos y garajes, o las actividades que se desarrollan desde los centros de control y otros puntos, zonas o áreas de las autopistas de peaje. Estas funciones podrán realizarse por personal distinto del de seguridad privada.

2. No se podrán utilizar cámaras o videocámaras con fines de seguridad privada para tomar imágenes y sonidos de vías y espacios públicos o de acceso público salvo en los supuestos y en los términos y condiciones previstos en su normativa específica, previa autorización administrativa por el órgano competente en cada caso. Su utilización en el interior de los domicilios requerirá el consentimiento del titular.

3. Las cámaras de videovigilancia que formen parte de medidas de seguridad obligatorias o de sistemas de recepción, verificación y, en su caso, respuesta y transmisión de alarmas, no requerirán autorización administrativa para su instalación, empleo o utilización.

4. Las grabaciones realizadas por los sistemas de videovigilancia no podrán destinarse a un uso distinto del de su finalidad. Cuando las mismas se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, se aportarán, de propia iniciativa o a su requerimiento, a las Fuerzas y Cuerpos de Seguridad competentes, respetando los criterios de conservación y custodia de las mismas para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales.

5. La monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los sistemas de videovigilancia estará sometida a lo previsto en la normativa en materia de protección de datos de carácter personal, y especialmente a los principios de proporcionalidad, idoneidad e intervención mínima.

6. En lo no previsto en la presente ley y en sus normas de desarrollo, se aplicará lo dispuesto en la normativa sobre videovigilancia por parte de las Fuerzas y Cuerpos de Seguridad.

[. . .]

CAPÍTULO III

Servicios de los despachos de detectives privados

Artículo 48. *Servicios de investigación privada.*

1. Los servicios de investigación privada, a cargo de detectives privados, consistirán en la realización de las averiguaciones que resulten necesarias para la obtención y aportación, por cuenta de terceros legitimados, de información y pruebas sobre conductas o hechos privados relacionados con los siguientes aspectos:

a) Los relativos al ámbito económico, laboral, mercantil, financiero y, en general, a la vida personal, familiar o social, exceptuada la que se desarrolle en los domicilios o lugares reservados.

b) La obtención de información tendente a garantizar el normal desarrollo de las actividades que tengan lugar en ferias, hoteles, exposiciones, espectáculos, certámenes, convenciones, grandes superficies comerciales, locales públicos de gran concurrencia o ámbitos análogos.

c) La realización de averiguaciones y la obtención de información y pruebas relativas a delitos sólo perseguibles a instancia de parte por encargo de los sujetos legitimados en el proceso penal.

2. La aceptación del encargo de estos servicios por los despachos de detectives privados requerirá, en todo caso, la acreditación, por el solicitante de los mismos, del interés legítimo alegado, de lo que se dejará constancia en el expediente de contratación e investigación que se abra.

3. En ningún caso se podrá investigar la vida íntima de las personas que transcurra en sus domicilios u otros lugares reservados, ni podrán utilizarse en este tipo de servicios medios personales, materiales o técnicos de tal forma que atenten contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones o a la protección de datos.

4. En la prestación de los servicios de investigación, los detectives privados no podrán utilizar o hacer uso de medios, vehículos o distintivos que puedan confundirse con los de las Fuerzas y Cuerpos de Seguridad.

5. En todo caso, los despachos de detectives y los detectives privados encargados de las investigaciones velarán por los derechos de sus clientes con respeto a los de los sujetos investigados.

6. Los servicios de investigación privada se ejecutarán con respeto a los principios de razonabilidad, necesidad, idoneidad y proporcionalidad.

Artículo 49. *Informes de investigación.*

1. Por cada servicio que les sea contratado, los despachos o los detectives privados encargados del asunto deberán elaborar un único informe en el que reflejarán el número de registro asignado al servicio, los datos de la persona que encarga y contrata el servicio, el objeto de la contratación, los medios, los resultados, los detectives intervinientes y las actuaciones realizadas, en las condiciones y plazos que reglamentariamente se establezcan.

2. En el informe de investigación únicamente se hará constar información directamente relacionada con el objeto y finalidad de la investigación contratada, sin incluir en él referencias, informaciones o datos que hayan podido averiguarse relativos al cliente o al sujeto investigado, en particular los de carácter personal especialmente protegidos, que no resulten necesarios o que no guarden directa relación con dicho objeto y finalidad ni con el interés legítimo alegado para la contratación.

3. Dicho informe estará a disposición del cliente, a quien se entregará, en su caso, al finalizar el servicio, así como a disposición de las autoridades policiales competentes para la inspección, en los términos previstos en el artículo 54.5.

4. Los informes de investigación deberán conservarse archivados, al menos, durante tres años, sin perjuicio de lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Las imágenes y los sonidos grabados durante las investigaciones se destruirán tres años después de su finalización, salvo que estén relacionadas con un procedimiento judicial, una investigación policial o un procedimiento sancionador. En todo caso, el tratamiento de dichas imágenes y sonidos deberá observar lo establecido en la normativa sobre protección de datos de carácter personal, especialmente sobre el bloqueo de datos previsto en la misma.

5. Las investigaciones privadas tendrán carácter reservado y los datos obtenidos a través de las mismas solo se podrán poner a disposición del cliente o, en su caso, de los órganos judiciales y policiales, en este último supuesto únicamente para una investigación policial o para un procedimiento sancionador, conforme a lo dispuesto en el artículo 25.

[. . .]

TÍTULO VI

Régimen sancionador

CAPÍTULO I

Infracciones

[. . .]

Artículo 57. *Infracciones de las empresas que desarrollen actividades de seguridad privada, de sus representantes legales, de los despachos de detectives privados y de las centrales de alarma de uso propio.*

Las empresas que desarrollen actividades de seguridad privada, sus representantes legales, los despachos de detectives privados y las centrales de alarma de uso propio, podrán incurrir en las siguientes infracciones:

1. Infracciones muy graves:

a) La prestación de servicios de seguridad privada a terceros careciendo de autorización o, en su caso, sin haber presentado la declaración responsable prevista en el artículo 18.1 y 2 para la prestación de los servicios de que se trate.

b) La contratación o utilización, en servicios de seguridad privada, de personas que carezcan de la habilitación o acreditación correspondiente.

c) La realización de actividades prohibidas en el artículo 8.4, sobre reuniones o manifestaciones, conflictos políticos o laborales, control de opiniones o su expresión, o la información a terceras personas sobre bienes de cuya seguridad o investigación hubieran sido encargados, o cualquier otra forma de quebrantamiento del deber de reserva, cuando no sean constitutivas de delito y salvo que sean constitutivas de infracción a la normativa sobre protección de datos de carácter personal.

d) La instalación o utilización de medios materiales o técnicos no homologados cuando la homologación sea preceptiva y sean susceptibles de causar grave daño a las personas o a los intereses generales.

e) La negativa a facilitar, cuando proceda, la información contenida en los contratos de seguridad privada, en los libros-registro o el acceso a los informes de investigación privada.

f) El incumplimiento de las previsiones normativas sobre adquisición y uso de armas, así como sobre disponibilidad de armeros y custodia de aquéllas, particularmente la tenencia de armas por el personal a su servicio fuera de los casos permitidos por esta ley, o la contratación de instructores de tiro que carezcan de la oportuna habilitación.

g) La prestación de servicios de seguridad privada con armas de fuego fuera de lo dispuesto en esta ley.

h) La negativa a prestar auxilio o colaboración a las Fuerzas y Cuerpos de Seguridad en la investigación y persecución de actos delictivos; en el descubrimiento y detención de los delincuentes; o en la realización de las funciones inspectoras o de control que les correspondan.

i) El incumplimiento de la obligación que impone a los representantes legales el artículo 22.3.

j) La ausencia de las medidas de seguridad obligatorias, por parte de las empresas de seguridad privada y los despachos de detectives, en sus sedes, delegaciones y sucursales.

k) El incumplimiento de las condiciones de prestación de servicios establecidos por la autoridad competente en relación con el ejercicio del derecho de huelga en servicios esenciales, o en los que el servicio de seguridad se haya impuesto obligatoriamente, en los supuestos a que se refiere el artículo 8.6.

l) El incumplimiento de los requisitos que impone a las empresas de seguridad el artículo 19. 1, 2 y 3, y el artículo 35.2.

m) El incumplimiento de los requisitos que impone a los despachos de detectives el artículo 24. 1 y 2.

n) La falta de transmisión a las Fuerzas y Cuerpos de Seguridad competentes de las alarmas reales que se registren en las centrales receptoras de alarmas privadas, incluidas las de uso propio, así como el retraso en la transmisión de las mismas, cuando estas conductas no estén justificadas.

ñ) La prestación de servicios compatibles contemplados en el artículo 6.2, empleando personal no habilitado que utilice armas o medios de defensa reservados al personal de seguridad privada.

o) La realización de investigaciones privadas a favor de solicitantes en los que no concurra un interés legítimo en el asunto.

p) La prestación de servicios de seguridad privada sin formalizar los correspondientes contratos.

q) El empleo o utilización, en servicios de seguridad privada, de medidas o de medios personales, materiales o técnicos de forma que se atente contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones, siempre que no constituyan delito.

r) La falta de comunicación por parte de empresas de seguridad informática de las incidencias relativas al sistema de cuya protección sean responsables cuando sea preceptivo.

s) La comisión de una tercera infracción grave o de una grave y otra muy grave en el período de dos años, habiendo sido sancionado por las anteriores.

t) La prestación de actividades ajenas a las de seguridad privada, excepto las compatibles previstas en el artículo 6 de la presente ley.

2. Infracciones graves:

a) La instalación o utilización de medios materiales o técnicos no homologados, cuando la homologación sea preceptiva.

b) La prestación de servicios de seguridad privada con vehículos, uniformes, distintivos, armas o medios de defensa que no reúnan las características reglamentarias.

c) La prestación de servicios de seguridad privada careciendo de los requisitos específicos de autorización o presentación de declaración responsable para la realización de dicho tipo de servicios. Esta infracción también será aplicable cuando tales servicios se lleven a cabo fuera del lugar o del ámbito territorial para el que estén autorizados o se haya presentado la declaración responsable, o careciendo de la autorización previa o de dicha declaración cuando éstas sean preceptivas, o cuando se realicen en condiciones distintas a las expresamente previstas en la autorización del servicio.

d) La retención de la documentación profesional del personal de seguridad privada, o de la acreditación del personal acreditado.

e) La prestación de servicios de seguridad privada sin comunicar correctamente los correspondientes contratos al Ministerio del Interior o al órgano autonómico competente, o en los casos en que la comunicación se haya producido con posterioridad al inicio del servicio.

f) La prestación de servicios de seguridad privada sin cumplir lo estipulado en el correspondiente contrato.

g) La falta de sustitución ante el abandono o la omisión injustificados del servicio por parte del personal de seguridad privada, dentro de la jornada laboral establecida.

h) La utilización, en el desempeño de funciones de seguridad privada, de personal de seguridad privada, con una antigüedad mínima de un año en la empresa, que no haya realizado los correspondientes cursos de actualización o especialización, no los haya superado, o no los haya realizado con la periodicidad que reglamentariamente se determine.

i) La falta de presentación al Ministerio del Interior o al órgano autonómico competente del certificado acreditativo de la vigencia del contrato de seguro, aval o seguro de caución en los términos establecidos en el artículo 19.1.e) y f) y 24.2.e) y f), así como la no presentación

del informe de actividades y el resumen de la cuenta anual a los que se refiere el artículo 21.1.e), o la no presentación de la memoria a la que se refiere el artículo 25.1.i)

j) La comunicación de una o más falsas alarmas por negligencia, deficiente funcionamiento o falta de verificación previa.

k) La apertura de delegaciones o sucursales sin obtener la autorización necesaria o sin haber presentado la declaración responsable ante el órgano competente, cuando sea preceptivo.

l) La falta de comunicación al Ministerio del Interior o, en su caso, al órgano autonómico competente, de las altas y bajas del personal de seguridad privada, así como de los cambios que se produzcan en sus representantes legales y toda variación en la composición personal de los órganos de administración, gestión, representación y dirección.

m) La prestación de servicio por parte del personal de seguridad privada sin la debida uniformidad o sin los medios que reglamentariamente sean exigibles.

n) La no realización de las revisiones anuales obligatorias de los sistemas o medidas de seguridad cuyo mantenimiento tuvieren contratado.

ñ) La carencia o falta de cumplimentación de cualquiera de los libros-registro obligatorios.

o) La falta de comunicación al Ministerio del Interior o, en su caso, al órgano autonómico competente de todo cambio relativo a su personalidad o forma jurídica, denominación, número de identificación fiscal o domicilio.

p) La falta de mantenimiento, en todo momento, de los requisitos establecidos para los representantes legales en el artículo 22.2.

q) El deficiente funcionamiento, por parte de las empresas de seguridad privada y despachos de detectives, en sus sedes, delegaciones o sucursales, de las medidas de seguridad obligatorias, así como el incumplimiento de las revisiones obligatorias de las mismas.

r) La prestación de servicios compatibles contemplados en el artículo 6.2 empleando personal no habilitado que utilice distintivos, uniformes o medios que puedan confundirse con los del personal de seguridad privada.

s) El incumplimiento de los requisitos impuestos a las empresas de seguridad informática.

t) La prestación de servicios incumpliendo lo dispuesto en el artículo 19.4.

u) La actuación de vigilantes de seguridad en el exterior de las instalaciones, inmuebles o propiedades de cuya vigilancia o protección estuvieran encargadas las empresas de seguridad privada con motivo de la prestación de servicios de tal naturaleza, fuera de los supuestos legalmente previstos.

v) No depositar la documentación profesional sobre contratos, informes de investigación y libros-registros en las dependencias del Cuerpo Nacional de Policía o, en su caso, del cuerpo de policía autonómico competente, en caso de cierre del despacho de detectives privados.

w) La comisión de una tercera infracción leve o de una grave y otra leve, en el período de dos años, habiendo recaído sanción por las anteriores.

x) La publicidad de servicios de seguridad privada por parte de personas, físicas o jurídicas, carentes de la correspondiente autorización o sin haber presentado declaración responsable.

y) La prestación de servicios de seguridad privada en condiciones distintas a las previstas en las comunicaciones de los correspondientes contratos.

3. Infracciones leves:

a) El incumplimiento de la periodicidad de las revisiones obligatorias de los sistemas o medidas de seguridad cuyo mantenimiento tuvieren contratado.

b) La utilización en los servicios de seguridad privada de vehículos, uniformes o distintivos con apariencia o semejanza a los de las Fuerzas y Cuerpos de Seguridad o de las Fuerzas Armadas.

c) La falta de diligencia en la cumplimentación de los libros-registro obligatorios.

d) En general, el incumplimiento de los trámites, condiciones o formalidades establecidos por esta ley, siempre que no constituya infracción grave o muy grave.

Artículo 58. *Infracciones del personal que desempeñe funciones de seguridad privada.*

El personal que desempeñe funciones de seguridad privada, así como los ingenieros, técnicos, operadores de seguridad y profesores acreditados, podrán incurrir en las siguientes infracciones:

1. Infracciones muy graves:

a) El ejercicio de funciones de seguridad privada para terceros careciendo de la habilitación o acreditación necesaria.

b) El incumplimiento de las previsiones contenidas en esta ley sobre tenencia de armas de fuego fuera del servicio y sobre su utilización.

c) La falta de reserva debida sobre los hechos que conozcan en el ejercicio de sus funciones o la utilización de medios materiales o técnicos de tal forma que atenten contra el derecho al honor, a la intimidad personal o familiar, a la propia imagen o al secreto de las comunicaciones cuando no constituyan delito.

d) La negativa a prestar auxilio o colaboración a las Fuerzas y Cuerpos de Seguridad, cuando sea procedente, en la investigación y persecución de actos delictivos; en el descubrimiento y detención de los delincuentes; o en la realización de las funciones inspectoras o de control que les correspondan.

e) La negativa a identificarse profesionalmente, en el ejercicio de sus respectivas funciones, ante la Autoridad o sus agentes, cuando fueren requeridos para ello.

f) La realización de investigaciones sobre delitos perseguibles de oficio o la falta de denuncia a la autoridad competente de los delitos que conozcan los detectives privados en el ejercicio de sus funciones.

g) La realización de actividades prohibidas en el artículo 8.4 sobre reuniones o manifestaciones, conflictos políticos y laborales, control de opiniones o su expresión, o la información a terceras personas sobre bienes de cuya seguridad estén encargados, en el caso de que no sean constitutivas de delito; salvo que sean constitutivas infracción a la normativa sobre protección de datos de carácter personal.

h) El ejercicio abusivo de sus funciones en relación con los ciudadanos.

i) La realización, orden o tolerancia, en el ejercicio de su actuación profesional, de prácticas abusivas, arbitrarias o discriminatorias, incluido el acoso, que entrañen violencia física o moral, cuando no constituyan delito.

j) El abandono o la omisión injustificados del servicio por parte del personal de seguridad privada, dentro de la jornada laboral establecida.

k) La elaboración de proyectos o ejecución de instalaciones o mantenimientos de sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, sin disponer de la acreditación correspondiente expedida por el Ministerio del Interior.

l) La no realización del informe de investigación que preceptivamente deben elaborar los detectives privados o su no entrega al contratante del servicio, o la elaboración de informes paralelos.

m) El ejercicio de funciones de seguridad privada por parte del personal a que se refiere el artículo 28.3 y 4.

n) La comisión de una tercera infracción grave o de una grave y otra muy grave en el período de dos años, habiendo sido sancionado por las anteriores.

2. Infracciones graves:

a) La realización de funciones de seguridad privada que excedan de la habilitación obtenida.

b) El ejercicio de funciones de seguridad privada por personal habilitado, no integrado en empresas de seguridad privada, o en la plantilla de la empresa, cuando resulte preceptivo conforme a lo dispuesto en el artículo 38.5, o al margen de los despachos de detectives.

c) La falta de respeto al honor o a la dignidad de las personas.

d) El ejercicio del derecho a la huelga al margen de lo dispuesto al respecto para los servicios que resulten o se declaren esenciales por la autoridad pública competente, o en los

que el servicio de seguridad se haya impuesto obligatoriamente, en los supuestos a que se refiere el artículo 8.6.

e) La no identificación profesional, en el ejercicio de sus respectivas funciones, cuando fueren requeridos para ello por los ciudadanos.

f) La retención de la documentación personal en contra de lo previsto en el artículo 32.1.b).

g) La falta de diligencia en el cumplimiento de las respectivas funciones por parte del personal habilitado o acreditado.

h) La identificación profesional haciendo uso de documentos o distintivos diferentes a los dispuestos legalmente para ello o acompañando éstos con emblemas o distintivos de apariencia semejante a los de las Fuerzas y Cuerpos de Seguridad o de las Fuerzas Armadas.

i) La negativa a realizar los cursos de formación permanente a los que vienen obligados.

j) La elaboración de proyectos o ejecución de instalaciones o mantenimientos de sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, no ajustados a las normas técnicas reglamentariamente establecidas.

k) La omisión, total o parcial, de los datos que obligatoriamente debe contener el informe de investigación que deben elaborar los detectives privados.

l) El ejercicio de funciones de seguridad privada incompatibles entre sí, por parte de personal habilitado para ellas.

m) La comisión de una tercera infracción leve o de una grave y otra leve, en el período de dos años, habiendo recaído sanción por las anteriores.

n) La validación provisional de sistemas o medidas de seguridad que no se adecuen a la normativa de seguridad privada.

3. Infracciones leves:

a) La actuación sin la debida uniformidad o medios, que reglamentariamente sean exigibles, o sin portar los distintivos o la documentación profesional, así como la correspondiente al arma de fuego utilizada en la prestación del servicio encomendado.

b) El trato incorrecto o desconsiderado con los ciudadanos.

c) La no cumplimentación, total o parcial, por parte de los técnicos acreditados, del documento justificativo de las revisiones obligatorias de los sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia.

d) En general, el incumplimiento de los trámites, condiciones o formalidades establecidos por esta ley, siempre que no constituya infracción grave o muy grave.

[. . .]

§ 33

Ley 26/2013, de 27 de diciembre, de cajas de ahorros y fundaciones bancarias. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 311, de 28 de diciembre de 2013
Última modificación: 27 de junio de 2014
Referencia: BOE-A-2013-13723

[. . .]

TÍTULO II

De las fundaciones bancarias

[. . .]

CAPÍTULO V

Régimen de control

[. . .]

Artículo 46. *Funciones del Banco de España.*

1. Sin perjuicio de lo previsto en el título VI de la Ley 26/1988, de 29 de julio, sobre Disciplina e Intervención de las Entidades de Crédito, corresponderá al Banco de España el control del cumplimiento de las normas contenidas en el capítulo IV de esta Ley desde el marco de sus competencias como autoridad responsable de la supervisión de la entidad de crédito participada y, en particular, valorando la influencia de la fundación bancaria sobre la gestión sana y prudente de la citada entidad, de conformidad con los criterios establecidos en el régimen de participaciones significativas previsto en el citado título VI de la Ley 26/1988, de 29 de julio, sobre Disciplina e Intervención de las Entidades de Crédito.

2. A los efectos de las funciones de supervisión asignadas en el apartado anterior, el Banco de España podrá:

a) Realizar las inspecciones y las comprobaciones que considere oportunas en el ejercicio de sus funciones.

b) Requerir a la fundación bancaria cuanta información resulte necesaria para desarrollar sus funciones.

El acceso a las informaciones y datos requeridos por el Banco de España se encuentra amparado por el artículo 11.2.a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

3. Asimismo, el Ministro de Economía y Competitividad, o el Banco de España con su habilitación expresa, podrá desarrollar las normas y modelos a que deberá sujetarse la contabilidad de las fundaciones bancarias.

Para el establecimiento y modificación de las señaladas normas y modelos será preceptivo el informe previo del Instituto de Contabilidad y Auditoría de Cuentas.

[. . .]

§ 34

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 295, de 10 de diciembre de 2013
Última modificación: 21 de diciembre de 2013
Referencia: BOE-A-2013-12887

[. . .]

TÍTULO I

Transparencia de la actividad pública

[. . .]

CAPÍTULO II

Publicidad activa

Artículo 5. *Principios generales.*

1. Los sujetos enumerados en el artículo 2.1 publicarán de forma periódica y actualizada la información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública.

2. Las obligaciones de transparencia contenidas en este capítulo se entienden sin perjuicio de la aplicación de la normativa autonómica correspondiente o de otras disposiciones específicas que prevean un régimen más amplio en materia de publicidad.

3. Serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15. A este respecto, cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos.

4. La información sujeta a las obligaciones de transparencia será publicada en las correspondientes sedes electrónicas o páginas web y de una manera clara, estructurada y entendible para los interesados y, preferiblemente, en formatos reutilizables. Se establecerán los mecanismos adecuados para facilitar la accesibilidad, la interoperabilidad, la calidad y la reutilización de la información publicada así como su identificación y localización.

Cuando se trate de entidades sin ánimo de lucro que persigan exclusivamente fines de interés social o cultural y cuyo presupuesto sea inferior a 50.000 euros, el cumplimiento de las obligaciones derivadas de esta Ley podrá realizarse utilizando los medios electrónicos

puestos a su disposición por la Administración Pública de la que provenga la mayor parte de las ayudas o subvenciones públicas percibidas.

5. Toda la información será comprensible, de acceso fácil y gratuito y estará a disposición de las personas con discapacidad en una modalidad suministrada por medios o en formatos adecuados de manera que resulten accesibles y comprensibles, conforme al principio de accesibilidad universal y diseño para todos.

[. . .]

CAPÍTULO III

Derecho de acceso a la información pública

[. . .]

Artículo 15. *Protección de datos personales.*

1. Si la información solicitada contuviera datos especialmente protegidos a los que se refiere el apartado 2 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.

Si la información incluyese datos especialmente protegidos a los que se refiere el apartado 3 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, o datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso sólo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquél estuviera amparado por una norma con rango de Ley.

2. Con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano.

3. Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal.

Para la realización de la citada ponderación, dicho órgano tomará particularmente en consideración los siguientes criterios:

a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.

c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos.

d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad.

4. No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas.

5. La normativa de protección de datos personales será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso.

[. . .]

TÍTULO III

Consejo de Transparencia y Buen Gobierno

Artículo 33. *Consejo de Transparencia y Buen Gobierno.*

1. Se crea el Consejo de Transparencia y Buen Gobierno como organismo público de los previstos en la disposición adicional décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. Estará adscrito al Ministerio de Hacienda y Administraciones Públicas.

2. El Consejo de Transparencia y Buen Gobierno tiene personalidad jurídica propia y plena capacidad de obrar. Actúa con autonomía y plena independencia en el cumplimiento de sus fines.

[. . .]

Artículo 36. *Comisión de Transparencia y Buen Gobierno.*

1. La Comisión de Transparencia y Buen Gobierno ejercerá todas las competencias que le asigna esta Ley, así como aquellas que les sean atribuidas en su normativa de desarrollo.

2. Dicha Comisión estará compuesta por:

a) El Presidente.
b) Un Diputado.
c) Un Senador.
d) Un representante del Tribunal de Cuentas.
e) Un representante del Defensor del Pueblo.
f) Un representante de la Agencia Española de Protección de Datos.
g) Un representante de la Secretaría de Estado de Administraciones Públicas.
h) Un representante de la Autoridad Independiente de Responsabilidad Fiscal.

3. La condición de miembro de la Comisión del Consejo de Transparencia y Buen Gobierno no exigirá dedicación exclusiva ni dará derecho a remuneración con excepción de lo previsto en el artículo siguiente.

4. Al menos una vez al año, la Comisión de Transparencia y Buen Gobierno convocará a los representantes de los organismos que, con funciones similares a las desarrolladas por ella, hayan sido creados por las Comunidades Autónomas en ejercicio de sus competencias. A esta reunión podrá ser convocado un representante de la Administración Local propuesto por la Federación Española de Municipios y Provincias.

[. . .]

Disposición adicional quinta. *Colaboración con la Agencia Española de Protección de Datos.*

El Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos adoptarán conjuntamente los criterios de aplicación, en su ámbito de actuación, de las reglas contenidas en el artículo 15 de esta Ley, en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma, de conformidad con lo dispuesto en esta Ley y en la Ley Orgánica 15/1999, de 13 de diciembre.

[. . .]

Información relacionada

- Véanse los Reales Decretos 415/2016, de 3 de noviembre, Ref. BOE-A-2016-10167, 424/2016, de 11 de noviembre, Ref. BOE-A-2016-10459 y 769/2017, de 28 de julio, Ref. BOE-A-2017-9012, por los que el Portal de la Transparencia pasa a depender del Ministerio de Hacienda y Función Pública.

§ 35

Ley Orgánica 3/2013, de 20 de junio, de protección de la salud del deportista y lucha contra el dopaje en la actividad deportiva. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 148, de 21 de junio de 2013
Última modificación: 18 de febrero de 2017
Referencia: BOE-A-2013-6732

[. . .]

TÍTULO II

De la salud y del dopaje de los deportistas con licencia deportiva

CAPÍTULO I

El dopaje en el ámbito del deporte con licencia deportiva

[. . .]

Artículo 15. *Personal habilitado para su realización y otras garantías.*

1. Los controles de dopaje que consistan en la extracción de sangre del deportista se realizarán siempre por un médico, por un facultativo especialista en análisis clínicos u otro tipo de personal sanitario cuyo título le otorgue dicha competencia, y que esté habilitado por la Agencia Española de Protección de la Salud en el Deporte para el desempeño de esta función. El resto de controles referentes a otros parámetros biológicos deberá hacerse en todo caso por personal debidamente habilitado por la Agencia.

La Agencia Española de Protección de la Salud en el Deporte y los órganos competentes de las Comunidades Autónomas podrán desarrollar un sistema de reconocimiento mutuo de habilitaciones mediante la suscripción de convenios específicos.

Asimismo podrá realizar dicha función el personal médico o sanitario que se encuentre habilitado por las Federaciones internacionales, por la Agencia Mundial Antidopaje o por las Agencias Nacionales Antidopaje de otros países con los que la Agencia Española de Protección de la Salud en el Deporte haya suscrito convenios de colaboración a tal efecto.

2. Para facilitar el descanso nocturno del deportista, dentro de la franja horaria comprendida entre las 23:00 y las 06:00 horas no se deberá iniciar la realización de controles de dopaje fuera de competición ni controles de salud.

No obstante, en casos debidamente justificados, y con pleno respeto al principio de proporcionalidad, será posible la realización de controles de dopaje fuera de competición siempre que en el momento de realizarlos se informe al deportista de las razones que justifican la no observancia de la limitación horaria establecida en el párrafo anterior.

La Agencia Española de Protección de la Salud en el Deporte velará en el ejercicio de sus funciones, para que las condiciones de realización de los controles de dopaje previstos en la presente Ley se realicen ajustándose al principio de mínima intervención y velando por la proporcionalidad respecto del descanso nocturno del deportista y la afección de los derechos y la intimidad de los deportistas.

3. Los deportistas serán informados en el momento de recibir la notificación del control y, en su caso, al iniciarse la recogida de la muestra, de los derechos y obligaciones que les asisten en relación con el citado control, de los trámites esenciales del procedimiento y de sus principales consecuencias, del tratamiento y cesión de los datos previstos en la presente Ley, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Entre los mismos se incluirá el derecho a no someterse a la prueba, sin perjuicio de lo dispuesto en el apartado siguiente.

La Agencia Española de Protección de la Salud en el Deporte establecerá un modelo normalizado de información para la recogida de las muestras en la realización de los controles de dopaje.

El desarrollo de los controles deberá realizarse con pleno respeto a los derechos fundamentales de los deportistas.

4. A los efectos de los procedimientos disciplinarios en materia de dopaje que se sigan por la infracción tipificada en la letra c) del apartado primero del artículo 22 de esta Ley, la negativa sin justificación válida a someterse a los controles, una vez documentada, constituirá prueba suficiente a los efectos de exigir la responsabilidad disciplinaria del deportista.

Se entiende por justificación válida la imposibilidad de acudir como consecuencia acreditada de lesión que le impida objetivamente someterse al control, o cuando la realización del control ponga en grave riesgo la salud del deportista.

5. El documento que acredite la negativa sin justificación válida a que se refiere el apartado anterior, realizada por el personal habilitado, será suficiente para iniciar el correspondiente procedimiento disciplinario sin perjuicio del derecho de defensa del interesado.

Artículo 16. *Obligaciones accesorias en materia de dopaje.*

1. Los clubes, organizaciones, grupos y demás entidades deportivas a la que se refiere el título III de la Ley 10/1990, de 15 de octubre, del Deporte, o que participen en actividades o competiciones deportivas organizadas en el marco de la citada Ley, están obligados a llevar un libro, debidamente registrado en la Agencia Española de Protección de la Salud en el Deporte y de cuya integridad exista garantía, en el que harán constar los tratamientos médicos y sanitarios que hayan prescrito sus facultativos a los deportistas bajo su dirección, siempre que aquellos autoricen dicha inscripción.

Dicho libro registro tendrá la consideración de documento sanitario a los efectos de acceso a la información que contiene, custodia y protección de datos.

La Agencia Española de Protección de la Salud en el Deporte podrá complementar o sustituir el libro registro por procedimientos centralizados de base de datos con utilización de las tecnologías de la información y la comunicación e identificación electrónica, como la firma digital y los sistemas de historia electrónica única y centralizada.

Los deportistas podrán exigir, en el momento de su inscripción en el libro, que se les entregue una copia del asiento u otro documento equivalente, en el que conste debidamente identificado el facultativo o profesional sanitario que, bajo su dirección, ha prescrito o realizado el tratamiento médico o sanitario, debiendo constar la fecha, la firma y el sello, en su caso, del profesional responsable de la atención sanitaria. También podrán solicitar que el dato en cuestión sea incorporado a su tarjeta de salud.

Cualquier procedimiento médico, terapéutico o sanitario que se vaya a prescribir o aplicar a un deportista sujeto al ámbito de aplicación de esta Ley y que se considere dopaje incluso si es objeto de una autorización de uso terapéutico deberá seguir un procedimiento de consentimiento informado que se regulará reglamentariamente y del que se guardará copia en el libro registro. Cada actuación sanitaria deberá ser refrendada por la firma del deportista como garantía de que se ha realizado dicha actuación y se ha autorizado el asiento en el libro registro.

2. Esta obligación alcanza a las Federaciones deportivas españolas cuando los deportistas se encuentren bajo su responsabilidad en el marco de las selecciones deportivas.

3. En los deportes individuales, esta obligación recaerá sobre el deportista o sobre la correspondiente Federación española en la forma en que se indica en el apartado anterior. Respecto de su cumplimentación se aplicarán las mismas normas que para los deportes de equipo.

[. . .]

CAPÍTULO III

Protección de la salud

[. . .]

Artículo 44. *Investigación.*

1. El Consejo Superior de Deportes, en colaboración con el Sistema Nacional de Salud y en el marco de los planes estatales de investigación, promoverá la investigación científica asociada a la práctica deportiva, a la aplicación de la actividad deportiva en el tratamiento y prevención de enfermedades y a la lucha contra el dopaje, atendiendo a las diferentes necesidades de mujeres, hombres y menores de edad, así como a las necesidades específicas por razón de discapacidad.

2. Para la mejor consecución de los fines de investigación, el Consejo Superior de Deportes promoverá la adhesión voluntaria de las sociedades científicas y de los centros y profesionales que se dediquen a la medicina deportiva, con el objeto de constituir una red de centros especializados en la materia, mediante la suscripción de los correspondientes convenios de colaboración.

3. La información que aporten cuantos compongan la red se utilizará para la reconfiguración y actualización del Plan de Apoyo a la Salud, con pleno respeto a la normativa de protección de datos de carácter personal.

[. . .]

CAPÍTULO IV

Del tratamiento de datos relativos al dopaje

Artículo 52. *De la responsabilidad de los empleados públicos.*

1. El personal que desempeñe las funciones de control del dopaje deberá guardar la confidencialidad y el secreto respecto de los asuntos que conozca por razón de su trabajo.

2. Los datos, informes o antecedentes obtenidos en el desarrollo de sus funciones sólo podrán utilizarse para los fines de control del dopaje y, en su caso, para la denuncia de hechos que puedan ser constitutivos de infracción administrativa o de delito. También podrán ser utilizados para estudios científicos, siempre que no se revele la identidad de las personas.

3. Con independencia de la responsabilidad que proceda, de acuerdo con la legislación específicamente aplicable, en particular en materia de protección de datos de carácter

personal, las infracciones en la custodia y, en su caso, la difusión de los datos relativos a los controles y procedimientos en materia de dopaje tienen la consideración de infracción muy grave a los efectos de la legislación de empleados públicos.

Asimismo, dichas conductas tendrán la consideración de incumplimiento contractual a que se refiere el artículo 54.2.d) del Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores respecto del personal laboral al servicio de las Administraciones Públicas y, en todo caso, tendrán la consideración de falta muy grave a los efectos de régimen disciplinario previsto en la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público o en la norma convencional que resulte de aplicación.

4. La determinación de estas responsabilidades corresponde a los órganos disciplinarios competentes en materia de función pública.

[. . .]

Artículo 54. *Autorización de cesión de datos.*

Los datos y ficheros relativos a los controles de dopaje podrán ser cedidos, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, a los organismos internacionales públicos o privados de los que España sea parte y que participen en la lucha contra el dopaje en el ámbito deportivo, en el marco de lo que dispongan los compromisos internacionales legalmente vinculantes asumidos por España, o para realizar estadísticas o estudios de investigación.

TÍTULO III

Políticas públicas de control y supervisión general de los productos que pueden utilizarse para el dopaje en la actividad deportiva

[. . .]

CAPÍTULO II

De las condiciones de utilización de los productos susceptibles de producir dopaje en la actividad deportiva

[. . .]

Artículo 63. *Sistema de información.*

1. La Agencia Española de Protección de la Salud en el Deporte y las Comunidades Autónomas crearán, en el marco del órgano de cooperación correspondiente, un sistema de información acerca de la protección de la salud y contra el dopaje en el ámbito del deporte, que garantice la disponibilidad de la información y la comunicación recíprocas entre las Administraciones Públicas con competencias en materia de deporte y actividad física. En el seno de dicho órgano se acordarán los objetivos y contenidos de la información.

2. El sistema de información permitirá conocer las sustancias susceptibles de producir dopaje y los métodos prohibidos en el deporte, los datos de los expedientes disciplinarios incoados y sancionados, con indicación de las sustancias detectadas y los análisis realizados en los distintos laboratorios e incorporará, como datos básicos, los relativos a población deportiva, recursos humanos y materiales, actividad desarrollada, farmacia y productos sanitarios, financiación y resultados obtenidos, así como las expectativas y opinión de los deportistas, todo ello desde una concepción integral de la lucha contra el dopaje en el deporte.

Asimismo, permitirá conocer los controles y demás pruebas realizadas al amparo de la protección de la salud del deportista e incorporará un Registro específico en el que se incluyan las sanciones en la materia de todas las Administraciones Públicas.

El sistema incluirá la variable de sexo en las estadísticas, encuestas y tomas de datos que se lleven a cabo en la población deportiva, y realizará un análisis diferenciado de las expectativas y opiniones de las mujeres y hombres, introduciendo indicadores de género.

3. Dentro del sistema de información, y oída la Agencia Española de Protección de Datos, se establecerá la definición y normalización de datos, la selección de indicadores y los requerimientos técnicos necesarios para la integración de la información, con el fin de lograr la máxima fiabilidad de la información que se produzca.

4. El sistema de información estará a disposición de sus usuarios, que serán las Administraciones Públicas deportivas y sanitarias, los gestores y profesionales del deporte y de la sanidad, así como la propia ciudadanía, en los términos de acceso y de difusión que se acuerden, previo informe de la Agencia Española de Protección de Datos. En todo caso, el sistema deberá facilitar la información en formatos adecuados, siguiendo el principio de diseño para todas las personas, de manera que resulten accesibles y comprensibles para las personas con discapacidad.

El acceso a los datos de los expedientes disciplinarios incoados y sancionados, con indicación de las sustancias detectadas y los análisis realizados en los distintos laboratorios, quedará siempre limitado a los órganos competentes en relación con dichos expedientes. El acceso por otras organizaciones, personas o entidades a dichos datos deberá ir siempre precedido de la disociación de los datos de carácter personal para cuantos intervengan en el expediente.

5. Las Comunidades Autónomas, la Administración General del Estado y las Entidades locales aportarán a este sistema de información los datos necesarios para su mantenimiento y desarrollo. Del mismo modo, la Administración General del Estado y las Comunidades Autónomas tienen derecho a acceder a los datos que formen parte del sistema de información, así como a disponer de ellos, en la medida en que, estrictamente, lo precisen para el ejercicio de sus competencias.

6. El tratamiento y la cesión de datos, incluidos aquellos de carácter personal necesarios para el sistema de información, estarán sujetos a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[. . .]

§ 36

Ley 4/2013, de 4 de junio, de medidas de flexibilización y fomento del mercado del alquiler de viviendas. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 134, de 5 de junio de 2013
Última modificación: sin modificaciones
Referencia: BOE-A-2013-5941

[. . .]

Artículo tercero. *Registro de sentencias firmes de impagos de rentas de alquiler.*

1. Se crea un Registro de sentencias firmes de impagos de rentas de alquiler. Por real decreto se regulará su organización y funcionamiento.

2. Con la finalidad de ofrecer información sobre el riesgo que supone arrendar inmuebles a personas que tienen precedentes de incumplimiento de sus obligaciones de pago de renta en contratos de arrendamiento y que, por dicho motivo, hayan sido condenadas por sentencia firme en un procedimiento de desahucio del artículo 250.1.1.° o del artículo 438 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, el secretario judicial correspondiente remitirá dicha información al Registro de sentencias firmes de impagos de rentas de alquiler.

3. En el mismo sentido, los órganos de arbitraje competentes deberán poner en conocimiento de dicho Registro los datos relativos a aquellas personas que hayan sido declaradas responsables del impago de rentas de arrendamientos, por medio de laudo arbitral dictado al efecto.

4. Tendrán acceso a la información obrante en el Registro, los propietarios de inmuebles que deseen suscribir contratos de arrendamiento sobre los mismos, sean personas físicas o jurídicas. A tales efectos deberán presentar una propuesta de contrato de arrendamiento en la que se identifique al eventual arrendatario, limitándose la información a la que tendrá derecho, a los datos que consten en el Registro, relacionados exclusivamente con dicho arrendatario.

5. Las personas incluidas en el Registro podrán instar la cancelación de la inscripción cuando en el proceso correspondiente hubieran satisfecho la deuda por la que fueron condenadas. No obstante, la constancia en el citado Registro tendrá una duración máxima de seis años, procediéndose a su cancelación automática a la finalización de dicho plazo.

6. La inscripción a la que se refiere este artículo estará, en todo caso sujeta a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Disposición adicional primera. *Transmisión de información sobre contratos de arrendamiento de vivienda.*

Con la finalidad de definir, proponer y ejecutar la política del Gobierno relativa al acceso a la vivienda, el Ministerio de Fomento podrá articular instrumentos de colaboración que le permitan obtener información acerca de la localización de las viviendas, de los contratos de arrendamiento sobre las mismas de los que se tenga constancia a través de los Registradores de la Propiedad, de los registros administrativos de contratos de arrendamiento o de depósitos de fianzas de las Comunidades Autónomas y del Consejo General del Notariado, así como de aquellos datos de carácter estadístico que consten en la Administración Tributaria derivados del acceso a beneficios fiscales de arrendadores y arrendatarios. En ningún caso, dicha información contendrá datos de carácter personal protegidos por la legislación en materia de protección de datos.

[. . .]

§ 37

Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 134, de 5 de junio de 2013
Última modificación: 28 de junio de 2017
Referencia: BOE-A-2013-5940

[. . .]

CAPÍTULO II

Funciones

[. . .]

Artículo 8. *Supervisión y control del mercado postal.*

La Comisión Nacional de los Mercados y la Competencia supervisará y controlará el correcto funcionamiento del mercado postal. En particular, ejercerá las siguientes funciones:

1. Velar para que se garantice el servicio postal universal, en cumplimiento de la normativa postal y la libre competencia en el sector, ejerciendo las funciones y competencias que le atribuye la legislación vigente, sin perjuicio de lo indicado en la Disposición adicional undécima de esta Ley.
2. Verificar la contabilidad analítica del operador designado y el coste neto del servicio postal universal y determinar la cuantía de la carga financiera injusta de la prestación de dicho servicio de conformidad con lo establecido en el Capítulo III del Título III de la Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal, así como en su normativa de desarrollo.
3. Gestionar el Fondo de financiación del servicio postal universal y las prestaciones de carácter público afectas a su financiación de conformidad con lo establecido en el Capítulo III del Título III de la Ley 43/2010, de 30 de diciembre, y en su normativa de desarrollo.
4. Supervisar y controlar la aplicación de la normativa vigente en materia de acceso a la red y a otras infraestructuras y servicios postales, de conformidad con lo establecido en el Título V de la Ley 43/2010, de 30 de diciembre, así como en su normativa de desarrollo.
5. Realizar el control y medición de las condiciones de prestación del servicio postal universal, de conformidad con lo establecido en el Capítulo II del Título III de la Ley 43/2010, de 30 de diciembre, así como en su normativa de desarrollo.

6. Gestionar y controlar la utilización del censo promocional conforme a lo definido en el artículo 31 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, conforme a lo que se determine reglamentariamente.

7. Dictar circulares para las entidades que operen en el sector postal, que serán vinculantes una vez publicadas en el «Boletín Oficial del Estado».

8. Emitir el informe previsto en la Disposición adicional segunda de la Ley 43/2010, de 30 de diciembre, para el seguimiento de las condiciones de prestación del servicio postal universal.

9. Realizar cualesquiera otras funciones que le sean atribuidas por Ley o por Real Decreto.

[. . .]

§ 38

Ley 33/2011, de 4 de octubre, General de Salud Pública. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 240, de 5 de octubre de 2011
Última modificación: 28 de marzo de 2014
Referencia: BOE-A-2011-15623

[. . .]

TÍTULO I

Derechos, deberes y obligaciones en salud pública

CAPÍTULO I

Derechos de los ciudadanos

[. . .]

Artículo 7. *Derecho a la intimidad, confidencialidad y respeto de la dignidad.*

1. Todas las personas tienen derecho al respeto de su dignidad e intimidad personal y familiar en relación con su participación en actuaciones de salud pública.

2. La información personal que se emplee en las actuaciones de salud pública se regirá por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en la Ley 41/2002, de 14 de noviembre, básica reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica.

[. . .]

CAPÍTULO IX

Sistema de Información en Salud Pública

[. . .]

Artículo 42. *Datos básicos y comunicación de la información.*

1. El Consejo Interterritorial del Sistema Nacional de Salud aprobará la información sobre salud pública que se incluya en el Sistema de Información en salud pública, a cuyo efecto definirá un conjunto de datos básicos en las condiciones y requisitos establecidos en el capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

2. El acceso a la información por parte de los usuarios del sistema se realizará en los términos establecidos en esta ley y sus disposiciones de desarrollo.

[. . .]

§ 39

Ley 29/2011, de 22 de septiembre, de Reconocimiento y Protección Integral a las Víctimas del Terrorismo. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 229, de 23 de septiembre de 2011
Última modificación: 6 de octubre de 2015
Referencia: BOE-A-2011-15039

[. . .]

TÍTULO CUARTO

Régimen de protección social

[. . .]

Artículo 42. *De la protección de datos y las limitaciones a la publicidad.*

En las actuaciones y procedimientos relacionados con el terrorismo, se protegerá la intimidad de las víctimas; en especial sus datos personales, los de sus descendientes y los de cualquier otra persona que esté bajo su guarda o custodia.

[. . .]

§ 40

Ley 26/2011, de 1 de agosto, de adaptación normativa a la Convención Internacional sobre los Derechos de las Personas con Discapacidad. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 184, de 2 de agosto de 2011
Última modificación: 31 de octubre de 2015
Referencia: BOE-A-2011-13241

[. . .]

Disposición adicional segunda. *Suministro de información de las Comunidades Autónomas.*

De acuerdo con los principios de información mutua y colaboración entre Administraciones públicas y con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y con el fin de garantizar el cumplimiento de las obligaciones previstas en tratados y convenios internacionales, las Comunidades Autónomas, en el ámbito de sus competencias, remitirán anualmente al Ministerio de Sanidad, Política Social e Igualdad, datos estadísticos sobre la situación de las personas con discapacidad, en la forma que se establezca reglamentariamente. La aportación de los datos relativos al empleo y a las condiciones de trabajo de las personas con discapacidad se regirá por su normativa específica.

[. . .]

§ 41

Ley 23/2011, de 29 de julio, de depósito legal. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 182, de 30 de julio de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-13114

[. . .]

CAPÍTULO I

Disposiciones generales

[. . .]

Artículo 2. *Objetivos del depósito legal.*

Son objetivos del depósito legal:

1. Recopilar, almacenar y conservar, en los centros de conservación de la Administración General del Estado y de las Comunidades Autónomas, las publicaciones que constituyen el patrimonio bibliográfico, sonoro, visual, audiovisual y digital español, con objeto de preservarlo y legarlo a las generaciones futuras, velar por su difusión y permitir el acceso al mismo para garantizar el derecho de acceso a la cultura, a la información y a la investigación.

2. Recoger la información precisa para confeccionar las estadísticas oficiales sobre el patrimonio de referencia.

3. Describir el conjunto de la producción bibliográfica, sonora, visual, audiovisual y digital española, con el fin de difundirla, y posibilitar el intercambio de datos con otras agencias o instituciones bibliotecarias españolas y extranjeras.

4. Permitir el acceso y la consulta de las publicaciones almacenadas, bien en las instalaciones de los propios centros de conservación o bien a través de bases de datos en línea de acceso restringido, asegurando su correcta conservación y respetando en todo caso la legislación sobre propiedad intelectual; protección de datos; de la lectura, del libro y de las bibliotecas; accesibilidad; así como lo dispuesto en esta ley.

[. . .]

CAPÍTULO II

De la obligación del depósito legal

[. . .]

Artículo 5. *Publicaciones excluidas del depósito legal.*

No serán objeto de depósito legal las siguientes publicaciones:

a) documentos de las Administraciones Públicas de carácter interno o que resulten susceptibles de integración en expedientes administrativos,

b) documentos de instituciones y organizaciones, incluidas las empresariales, que versen únicamente sobre asuntos internos y estén dirigidas al personal de las mismas, tales como circulares, instrucciones o manuales de procedimiento,

c) publicaciones destinadas a concursos de promoción o traslado de los cuerpos o escalas de las distintas administraciones públicas,

d) sellos de correo,

e) impresos de carácter social como invitaciones de boda y bautizo, esquelas de defunción, tarjetas de visita, carnés de identidad, títulos o diplomas,

f) impresos de oficinas, formularios, incluidos los oficiales, cuestionarios y encuestas no cumplimentadas excepto que complementen una obra cuyo contenido sea técnico o científico, por ejemplo, un volumen formado por una recopilación de formularios que acompaña a un libro sobre procedimiento administrativo,

g) publicaciones de impresión bajo demanda,

h) dossieres de prensa,

i) hojas comerciales publicitarias,

j) catálogos comerciales de todo tipo,

k) calendarios y agendas,

l) objetos tridimensionales, aunque acompañen a un documento principal,

m) manuales de instrucciones de objetos, electrodomésticos, maquinaria, o análogos,

n) todo producto de un sistema informático que contenga datos que afecten a la privacidad de personas físicas y jurídicas y cuantos estén incluidos en la normativa de protección de datos personales, y

ñ) programas audiovisuales emitidos por prestadores del servicio de comunicación audiovisual, salvo que sean objeto de distribución.

[. . .]

Artículo 8. *Sujetos obligados a constituir el depósito legal en el caso de documentos electrónicos y sitios web.*

1. La responsabilidad del depósito legal de los documentos electrónicos a los que se refiere el artículo 4 de la presente ley recaerá en su editor o productor.

2. Se habilita a los centros de conservación, tanto de titularidad estatal como autonómica, a detectar y reproducir documentos electrónicos que hayan sido objeto de comunicación pública y los sitios web libremente accesibles a través de redes de comunicaciones que puedan resultar de interés para los fines del depósito legal, respetando en todo caso la legislación sobre protección de datos y propiedad intelectual. Se exonera a los editores de sitios web a los que se refiere el artículo 4 de la presente ley del deber de depósito legal.

[. . .]

§ 42

Ley Orgánica 9/2011, de 27 de julio, de derechos y deberes de los miembros de las Fuerzas Armadas. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 180, de 28 de julio de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-12961

[. . .]

TÍTULO I

Del ejercicio de los derechos fundamentales y libertades públicas

[. . .]

Artículo 10. *Derecho a la intimidad y dignidad personal.*

1. El militar tiene derecho a la intimidad personal. En el ejercicio y salvaguarda de este derecho se tendrán en cuenta las circunstancias en que tengan lugar las operaciones.

También tiene derecho al secreto de las comunicaciones y a la inviolabilidad del domicilio, incluido el ubicado dentro de unidades, en los términos establecidos en la Constitución y en el resto del ordenamiento jurídico.

Se deberá respetar la dignidad personal y en el trabajo de todo militar, especialmente frente al acoso, tanto sexual y por razón de sexo como profesional.

2. Las revistas e inspecciones deberán respetar en todo caso los derechos contenidos en el apartado anterior.

Como norma general, el registro personal de los militares, de sus taquillas, efectos y pertenencias que estuvieren en la unidad requerirá del consentimiento del afectado o resolución judicial. No obstante, cuando existan indicios de la comisión de un hecho delictivo o por razones fundadas de salud pública o de seguridad, el jefe de la unidad podrá autorizar tales registros de forma proporcionada y expresamente motivada. Estos registros se realizarán con la asistencia del interesado y en presencia de al menos dos testigos o sólo de éstos, si el interesado debidamente notificado no asistiera.

3. Los datos relativos a los miembros de las Fuerzas Armadas estarán sujetos a la legislación sobre protección de datos de carácter personal. A tal efecto los poderes públicos llevarán a cabo las acciones necesarias para la plena efectividad de este derecho fundamental, especialmente cuando concurran circunstancias que pudieran incidir en la seguridad de los militares.

[. . .]

§ 43

Ley 20/2011, de 21 de julio, del Registro Civil. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 175, de 22 de julio de 2011
Última modificación: 12 de junio de 2018
Referencia: BOE-A-2011-12628

[. . .]

TÍTULO I

El Registro Civil. Disposiciones generales

CAPÍTULO PRIMERO

Naturaleza, contenido y competencias del Registro Civil

[. . .]

Artículo 3. *Elementos definitorios del Registro Civil.*

1. El Registro Civil es único para toda España.

2. El Registro Civil es electrónico. Los datos serán objeto de tratamiento automatizado y se integrarán en una base de datos única cuya estructura, organización y funcionamiento es competencia del Ministerio de Justicia conforme a la presente Ley y a sus normas de desarrollo.

3. Serán de aplicación al Registro Civil las medidas de seguridad establecidas en la normativa vigente en materia de protección de datos de carácter personal.

[. . .]

Disposición adicional novena. *Obtención de datos del Instituto Nacional de Estadística.*

Para facilitar la tramitación telemática a los Registros Civiles, el Instituto Nacional de Estadística dará acceso telemático a los datos de domicilio relativos al Padrón municipal que guarden relación con los hechos inscribibles, así como, si fuera necesario para la correcta identificación de los citados hechos, a los datos de identificación que figuren en las inscripciones padronales, sin precisar para todo ello del consentimiento del interesado.

También se utilizarán los datos padronales para la actualización de la información obrante en las bases de datos de los Registros Civiles, en idénticas condiciones que en el párrafo anterior.

[. . .]

Disposición final quinta bis. *Aranceles notariales.*

El Gobierno aprobará los aranceles correspondientes a la intervención de los Notarios en la tramitación de las actas matrimoniales previas y por la celebración de matrimonios en forma civil con la autorización de las escrituras públicas correspondientes.

[. . .]

§ 44

Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 160, de 6 de julio de 2011
Última modificación: 6 de octubre de 2015
Referencia: BOE-A-2011-11605

[. . .]

TÍTULO II

Uso de los medios electrónicos en la Administración de Justicia

CAPÍTULO I

Derechos de los ciudadanos en sus relaciones con la Administración de Justicia por medios electrónicos

Artículo 4. *Derechos de los ciudadanos.*

1. Los ciudadanos tienen derecho a relacionarse con la Administración de Justicia utilizando medios electrónicos para el ejercicio de los derechos previstos en los Capítulos I y VII del Título III del Libro III de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, en la forma y con las limitaciones que en los mismos se establecen.

2. Además, los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad judicial, y en los términos previstos en la presente Ley, los siguientes derechos:

a) A elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con la Administración de Justicia.

b) A la igualdad en el acceso electrónico a los servicios de la Administración de Justicia.

c) A conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean parte procesal legítima, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

d) A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de parte o acrediten interés legítimo, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

e) A la conservación en formato electrónico por la Administración de Justicia de los documentos electrónicos que formen parte de un expediente conforme a la normativa vigente en materia de archivos judiciales.

f) A utilizar los sistemas de identificación y firma electrónica del documento nacional de identidad o cualquier otro reconocido para cualquier trámite electrónico con la Administración de Justicia en los términos establecidos por las leyes procesales.

g) A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de la Administración de Justicia en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

h) A la calidad de los servicios públicos prestados por medios electrónicos.

i) A elegir las aplicaciones o sistemas para relacionarse con la Administración de Justicia siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos y, en todo caso, siempre que sean compatibles con los que dispongan los juzgados y tribunales y se respeten las garantías y requisitos previstos en el procedimiento que se trate.

[. . .]

CAPÍTULO II

Derechos y deberes de los profesionales de la justicia en sus relaciones con la Administración de Justicia por medios electrónicos

Artículo 6. *Derechos y deberes de los profesionales del ámbito de la justicia.*

1. Los profesionales de la justicia tienen el derecho a relacionarse con la misma a través de medios electrónicos.

2. Además, los profesionales tienen, en relación con la utilización de los medios electrónicos en la actividad judicial y en los términos previstos en la presente Ley, los siguientes derechos:

a) A acceder y conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean representantes procesales de la parte personada, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

b) A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que sean representantes procesales de la parte personada o acrediten interés legítimo, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

c) A la conservación en formato electrónico por la Administración de Justicia de los documentos electrónicos que formen parte de un expediente según la normativa vigente en materia de archivos judiciales.

d) A utilizar los sistemas de firma electrónica del Documento Nacional de Identidad o cualquier otro reconocido, siempre que dicho sistema le identifique de forma unívoca como profesional para cualquier trámite electrónico con la Administración en los términos establecidos por las leyes procesales.

A tal efecto, el Consejo General o el superior correspondiente deberá poner a disposición de las oficinas judiciales los protocolos y sistemas de interconexión que permitan el acceso necesario por medios electrónicos al registro de profesionales colegiados ejercientes previsto en el artículo 10 de la Ley 2/1974, de 13 de febrero, sobre los Colegios Profesionales, garantizando que en él consten sus datos profesionales, tales como número de colegiado, domicilio profesional, número de teléfono y de fax y dirección de correo electrónico.

e) A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de la Administración de Justicia en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de

carácter personal, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

3. Los profesionales de la justicia, en los términos previstos en la presente Ley, tienen el deber de utilizar los medios electrónicos, las aplicaciones o los sistemas establecidos por las Administraciones competentes en materia de justicia, respetando en todo caso las garantías y requisitos previstos en el procedimiento que se trate.

[. . .]

CAPÍTULO III

Utilización obligatoria de los medios electrónicos en la tramitación de los procedimientos electrónicos judiciales

[. . .]

TÍTULO III

Régimen jurídico de la Administración judicial electrónica

CAPÍTULO I

De la sede judicial electrónica

[. . .]

Artículo 11. *Contenido y servicios de las sedes judiciales electrónicas.*

1. Toda sede judicial electrónica dispondrá, al menos, de los siguientes contenidos:

a) Identificación de la sede, así como del órgano u órganos titulares y de los responsables de la gestión, de los servicios puestos a disposición en la misma y, en su caso, de las subsedes de ella derivadas.

b) Información necesaria para su correcta utilización, incluyendo el mapa de la sede judicial electrónica o información equivalente, con especificación de la estructura de navegación y las distintas secciones disponibles.

c) Sistema de verificación de los certificados de la sede, que estará accesible de forma directa y gratuita.

d) Relación de sistemas de firma electrónica que, conforme a lo previsto en esta Ley, sean admitidos o utilizados en la sede.

e) Normas de creación del registro o registros electrónicos accesibles desde la sede.

f) Información relacionada con la protección de datos de carácter personal, incluyendo un enlace con la sede electrónica de la Agencia Española de Protección de Datos y las de las Agencias Autonómicas de Protección de Datos.

2. Las sedes judiciales electrónicas dispondrán, al menos, de los siguientes servicios a disposición de los ciudadanos y profesionales:

a) La relación de los servicios disponibles en la sede judicial electrónica.

b) La carta de servicios y la carta de servicios electrónicos.

c) La relación de los medios electrónicos que los ciudadanos y profesionales pueden utilizar en cada supuesto en el ejercicio de su derecho a comunicarse con la Administración de Justicia.

d) Un enlace para la formulación de sugerencias y quejas ante los órganos correspondientes.

e) Acceso, en los términos legalmente establecidos, al estado de tramitación del expediente.

f) Publicación electrónica, cuando proceda, de resoluciones y comunicaciones que deban publicarse en tablón de anuncios o edictos.

g) Verificación de los sellos electrónicos de los órganos u organismos públicos que abarque la sede.

h) Comprobación de la autenticidad e integridad de los documentos emitidos por los órganos u organismos públicos que abarca la sede que hayan sido autenticados mediante código seguro de verificación.

i) Servicios de asesoramiento electrónico al usuario para la correcta utilización de la sede.

j) La Carta de Derechos de los Ciudadanos ante la Justicia.

3. No será necesario recoger en las subsedes la información y los servicios a que se refieren los apartados anteriores cuando ya figuren en la sede de la que aquéllas derivan.

4. La sede judicial electrónica garantizará el régimen de cooficialidad lingüística vigente en su territorio.

[. . .]

TÍTULO IV

De la tramitación electrónica de los procedimientos judiciales

[. . .]

CAPÍTULO II

Del expediente judicial electrónico

[. . .]

Artículo 29. *Archivo electrónico de documentos.*

1. Podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones judiciales.

Los Archivos Judiciales de Gestión, Territoriales y Central serán gestionados mediante programas y aplicaciones informáticas, compatibles con los ya existentes en juzgados y tribunales, adaptados a las funciones y cometidos de cada uno, cuyo funcionamiento electrónico será regulado mediante Real Decreto.

2. Los documentos electrónicos que contengan actos procesales que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

3. Los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados y ajustarse a los requerimientos que garanticen la compatibilidad e interoperabilidad de los sistemas informáticos. En particular, asegurarán la identificación de los usuarios y el control de accesos, el cumplimiento de las garantías previstas en la legislación de protección de datos, así como lo previsto en los artículos 234 y 235 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

4. Sin perjuicio de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, el Consejo General del Poder Judicial regulará

reglamentariamente la reutilización de sentencias y otras resoluciones judiciales por medios digitales de referencia o reenvío de información, sea o no con fines comerciales, por parte de personas físicas o jurídicas para facilitar el acceso a las mismas de terceras personas.

CAPÍTULO III

Del registro de escritos, las comunicaciones y las notificaciones electrónicas

[. . .]

Artículo 32 bis. *Archivos electrónicos de apoderamientos apud acta.*

1. Asimismo, se dispondrá en las oficinas judiciales con funciones de registro, de un archivo electrónico de apoderamientos en el que deberán inscribirse los apoderamientos apud acta otorgados presencial o electrónicamente por quien ostente la condición de interesado en un procedimiento judicial a favor de representante, para actuar en su nombre ante la Administración de Justicia.

Ello no impedirá la existencia de archivos electrónicos de apoderamientos apud acta en cada oficina judicial para la realización de los trámites específicos en cada una.

2. Los archivos electrónicos de apoderamientos apud acta deberán ser plenamente interoperables entre sí, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se registren en sus correspondientes archivos.

Los archivos electrónicos de apoderamientos apud acta permitirán comprobar válidamente la representación que ostentan quienes actúen ante la Administración de Justicia en nombre de un tercero.

3. Los asientos que se realicen en los archivos electrónicos de apoderamientos apud acta deberán contener, al menos, la siguiente información:

a) Nombre y apellidos o razón social, número de documento nacional de identidad, de identificación fiscal o de documento equivalente del poderdante.

b) Nombre y apellidos o razón social, número de documento nacional de identidad, de identificación fiscal o de documento equivalente del apoderado.

c) Fecha de inscripción.

d) Tipo de poder según las facultades que otorgue.

4. Los apoderamientos apud acta que se inscriban en los archivos electrónicos de apoderamientos apud acta deberán corresponder a alguna de las siguientes tipologías:

a) Un poder general para que el apoderado pueda actuar en nombre del poderdante en cualquier actuación judicial.

b) Un poder para que el apoderado pueda actuar en nombre del poderdante únicamente en determinadas clases de procedimientos.

c) Un poder especial para que el apoderado pueda actuar en nombre del poderdante en un procedimiento concreto.

5. El poder inscribible en que la parte otorgue su representación al apoderado habrá de ser conferido por comparecencia apud acta.

El apoderamiento apud acta se otorgará mediante comparecencia electrónica en la correspondiente sede electrónica judicial haciendo uso de los sistemas de firma electrónica previstos en esta Ley, o bien mediante comparecencia personal ante el secretario judicial de cualquier oficina judicial.

6. Los apoderamientos inscritos en el archivo tendrán una validez determinada máxima de cinco años a contar desde la fecha de inscripción. En todo caso, en cualquier momento antes de la finalización de dicho plazo el poderdante podrá revocar o prorrogar el poder. Las prórrogas otorgadas por el poderdante al apoderamiento tendrán una validez determinada máxima de cinco años a contar desde la fecha de inscripción.

7. Las solicitudes de revocación, de prórroga o de denuncia del mismo podrán dirigirse a cualquier archivo, debiendo quedar inscrita esta circunstancia en el archivo ante el que tenga efectos el poder y surtiendo efectos desde la fecha en la que se produzca dicha inscripción.

Sección 2.ª De las comunicaciones y las notificaciones electrónicas

Artículo 33. *Comunicaciones electrónicas.*

1. Los ciudadanos podrán elegir en todo momento la manera de comunicarse con la Administración de Justicia, sea o no por medios electrónicos.

Asimismo, se podrá establecer legal o reglamentariamente la obligatoriedad de comunicarse con ella utilizando solo medios electrónicos cuando se trate de personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos.

2. Las comunicaciones a través de medios electrónicos se realizarán, en todo caso, con sujeción a lo dispuesto en la legislación procesal y serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas y del contenido íntegro de las comunicaciones, y se identifique con la autenticación que sea exigible al remitente y al destinatario de las mismas.

3. Las Administraciones competentes en materia de justicia publicarán, en el correspondiente «Diario Oficial» y en la propia sede judicial electrónica, aquellos medios electrónicos que los ciudadanos pueden utilizar en cada supuesto en el ejercicio de su derecho a comunicarse con las oficinas judiciales.

4. Los requisitos de seguridad e integridad de las comunicaciones se establecerán en cada caso de forma apropiada al carácter de los datos objeto de aquellas, de acuerdo con criterios de proporcionalidad, conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal y en las leyes procesales.

5. Los profesionales de la justicia deberán realizar sus comunicaciones por medios electrónicos cuando técnicamente estén disponibles.

6. Las oficinas judiciales utilizarán en todo caso medios electrónicos en sus comunicaciones con otras Administraciones y organismos públicos, salvo imposibilidad legal o material.

[. . .]

CAPÍTULO IV

De la tramitación electrónica

[. . .]

Artículo 41. *Acceso de las partes a la información sobre el estado de tramitación.*

Se pondrá a disposición de las partes un servicio electrónico de acceso restringido donde éstas puedan consultar, previa identificación y autenticación, al menos la información sobre el estado de tramitación del procedimiento, salvo que la normativa aplicable establezca restricciones a dicha información y con pleno respeto a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, y legislación que la desarrolla. La información sobre el estado de tramitación del procedimiento comprenderá la relación de los actos de trámite realizados, con indicación sobre su contenido, así como la fecha en la que fueron dictados.

[. . .]

TÍTULO V

Cooperación entre las Administraciones con competencias en materia de Administración de Justicia. El Esquema judicial de interoperabilidad y seguridad

CAPÍTULO I

Marco institucional de cooperación en materia de administración electrónica

Artículo 44. *El Comité técnico estatal de la Administración judicial electrónica.*

1. El Comité técnico estatal de la Administración judicial electrónica estará integrado por una representación del Ministerio de Justicia y de cada una de las Comunidades Autónomas con competencias en la materia y por los representantes que al efecto podrán designar el Consejo General del Poder Judicial y la Fiscalía General del Estado.

Este Comité técnico estará copresidido por un representante del Consejo General del Poder Judicial y otro del Ministerio de Justicia.

2. Sin perjuicio de las competencias del Consejo General del Poder Judicial como garante de la compatibilidad de sistemas informáticos, este Comité tendrá las siguientes funciones:

a) Favorecer la compatibilidad y asegurar la interoperabilidad de los sistemas y aplicaciones empleados por la Administración de Justicia.

b) Preparar planes y programas conjuntos de actuación para impulsar el desarrollo de la Administración judicial electrónica, respetando en todo caso las competencias autonómicas atinentes a los medios materiales de la Administración de Justicia.

c) Promover la cooperación de otras Administraciones públicas con la Administración de Justicia para suministrar a los órganos judiciales, a través de las plataformas de interoperabilidad establecidas por el Consejo General del Poder Judicial y por las Administraciones competentes en materia de Administración de Justicia, la información que precisen en el curso de un proceso judicial en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y en las leyes procesales.

d) Aquellas otras que legalmente se determinen.

[. . .]

Disposición adicional primera. *Creación del Comité técnico estatal de la Administración judicial electrónica.*

La estructura, composición y funciones del Comité técnico estatal de la Administración judicial electrónica serán establecidas reglamentariamente por el Gobierno, mediante Real Decreto, previo informe del Consejo General del Poder Judicial, de la Fiscalía General del Estado, de la Agencia Española de Protección de Datos y de las Comunidades Autónomas con competencias en la materia.

[. . .]

§ 45

Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 131, de 2 de junio de 2011
Última modificación: 7 de octubre de 2017
Referencia: BOE-A-2011-9617

[. . .]

TÍTULO II

Recursos humanos dedicados a la investigación

CAPÍTULO I

Personal Investigador al servicio de las Universidades públicas, de los Organismos Públicos de Investigación y de los Organismos de investigación de otras Administraciones Públicas

[. . .]

Artículo 15. *Deberes del personal investigador.*

1. Los deberes del personal investigador que preste servicios en Universidades públicas, en Organismos Públicos de Investigación de la Administración General del Estado o en Organismos de investigación de otras Administraciones Públicas serán los siguientes:

a) Observar las prácticas éticas reconocidas y los principios éticos correspondientes a sus disciplinas, así como las normas éticas recogidas en los diversos códigos deontológicos aplicables.

b) Poner en conocimiento de las entidades para las que presta servicios todos los hallazgos, descubrimientos y resultados susceptibles de protección jurídica, y colaborar en los procesos de protección y de transferencia de los resultados de sus investigaciones.

c) Difundir los resultados de sus investigaciones, en su caso, según lo indicado en esta ley.

d) Participar en las reuniones y actividades de los órganos de gobierno y de gestión de los que forme parte, y en los procesos de evaluación y mejora para los que se le requiera.

e) Procurar que su labor sea relevante para la sociedad.

f) Adoptar las medidas necesarias para evitar el plagio.

g) Encaminar sus investigaciones hacia el logro de los objetivos estratégicos de las entidades para las que presta servicios, y obtener o colaborar en los procesos de obtención de los permisos y autorizaciones necesarias antes de iniciar su labor.

h) Informar a las entidades para las que presta servicios o que financian o supervisan su actividad de posibles retrasos y redefiniciones en los proyectos de investigación de los que sea responsable, así como de la finalización de los proyectos, o de la necesidad de abandonar o suspender los proyectos antes de lo previsto.

i) Rendir cuentas sobre su trabajo a las entidades para las que presta servicios o que financian o supervisan su actividad, y responsabilizarse del uso eficaz de la financiación de los proyectos de investigación que desarrolle. Para ello, deberá observar los principios de gestión financiera correcta, transparente y eficaz, y cooperar en las auditorías sobre sus investigaciones que procedan según la normativa vigente.

j) Utilizar la denominación de las entidades para las que presta servicios en la realización de su actividad científica, de acuerdo con la normativa interna de dichas entidades y los acuerdos, pactos y convenios que éstas suscriban.

k) Seguir en todo momento prácticas de trabajo seguras de acuerdo con la normativa aplicable, incluida la adopción de las precauciones necesarias en materia de prevención de riesgos laborales, y velar por que el personal a su cargo cumpla con estas prácticas.

l) Adoptar las medidas necesarias para el cumplimiento de la normativa aplicable en materia de protección de datos y de confidencialidad.

2. Estos deberes se entenderán sin perjuicio de los establecidos por la Ley 7/2007, de 12 de abril, así como de los restantes deberes que resulten de aplicación al personal investigador, en función del tipo de entidad para la que preste servicios y de la actividad realizada.

[. . .]

CAPÍTULO II

Especificidades aplicables al personal al servicio de los Organismos Públicos de Investigación de la Administración General del Estado

[. . .]

Sección 2.ª Personal de investigación al servicio de los organismos públicos de Investigación de la Administración General del Estado

[. . .]

Artículo 28. *Derechos y deberes del personal técnico al servicio de los Organismos Públicos de Investigación de la Administración General del Estado.*

1. Serán de aplicación al personal técnico al servicio de los Organismos Públicos de Investigación de la Administración General del Estado los artículos 16.1 y 2 de esta ley. Además, serán de aplicación al personal técnico funcionario de carrera o laboral fijo al servicio de los Organismos Públicos de Investigación de la Administración General del Estado los artículos 17, 18 y 19 de esta ley.

2. El personal técnico que preste servicios en Organismos Públicos de Investigación de la Administración General del Estado tendrá los siguientes derechos:

a) A determinar libremente los métodos de resolución de problemas, dentro del marco de las prácticas y los principios éticos reconocidos y de la normativa aplicable sobre propiedad intelectual, y teniendo en cuenta las posibles limitaciones derivadas de las circunstancias de la actividad y del entorno, de las actividades de supervisión, orientación o gestión, de las limitaciones presupuestarias o de las infraestructuras.

b) A ser reconocido y amparado en la autoría o coautoría de los trabajos de carácter técnico en los que participe.

c) Al respeto al principio de igualdad de género en el desempeño de sus funciones, en la contratación de personal y en el desarrollo de su carrera profesional.

d) A contar con los medios e instalaciones adecuados para el desarrollo de sus funciones, dentro de los límites derivados de la aplicación de los principios de eficacia y eficiencia en la asignación, utilización y gestión de dichos medios e instalaciones por la entidad para la que preste servicios, y dentro de las disponibilidades presupuestarias.

e) A la consideración y respeto de su actividad.

f) A utilizar la denominación de las entidades para las que presta servicios en la realización de su actividad.

g) A participar en los beneficios que obtengan las entidades para las que presta servicios, como consecuencia de la eventual explotación de los resultados de la actividad en que haya participado el personal técnico. Los referidos beneficios no tendrán en ningún caso naturaleza retributiva o salarial para el personal técnico.

h) A participar en los programas favorecedores de la conciliación entre la vida personal, familiar y laboral que pongan en práctica las entidades para las que presta servicios.

i) A su desarrollo profesional, mediante el acceso a medidas de formación continua para el desarrollo de sus capacidades y competencias.

Estos derechos se entenderán sin perjuicio de los establecidos por la Ley 7/2007, de 12 de abril, así como de los restantes derechos que resulten de aplicación al personal técnico, en función del tipo de entidad para la que preste servicios y de la actividad realizada.

3. Los deberes del personal técnico que preste servicios en Organismos Públicos de Investigación de la Administración General del Estado serán los siguientes:

a) Observar las prácticas éticas reconocidas y los principios éticos correspondientes a sus disciplinas, así como las normas éticas recogidas en los diversos códigos deontológicos aplicables.

b) Poner en conocimiento de las entidades para las que presta servicios todos los hallazgos, descubrimientos y resultados susceptibles de protección jurídica, y colaborar en los procesos de protección y de transferencia de los resultados de su actividad.

c) Participar en las reuniones y actividades de los órganos de gobierno y de gestión de los que forme parte y en los procesos de evaluación y mejora para los que se le requiera.

d) Procurar que su labor sea relevante para la sociedad.

e) Utilizar la denominación de las entidades para las que presta servicios en la realización de su actividad, de acuerdo con la normativa interna de dichas entidades y los acuerdos, pactos y convenios que éstas suscriban.

f) Seguir en todo momento prácticas de trabajo seguras de acuerdo con la normativa aplicable, incluida la adopción de las precauciones necesarias en materia de prevención de riesgos laborales, y velar por que el personal a su cargo cumpla con estas prácticas.

g) Adoptar las medidas necesarias para el cumplimiento de la normativa aplicable en materia de protección de datos y de confidencialidad.

Estos deberes se entenderán sin perjuicio de los establecidos por la Ley 7/2007, de 12 de abril, así como de los restantes deberes que resulten de aplicación al personal técnico, en función del tipo de entidad para la que preste servicios y de la actividad realizada.

[. . .]

§ 46

Ley 13/2011, de 27 de mayo, de regulación del juego. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 127, de 28 de mayo de 2011
Última modificación: 4 de julio de 2018
Referencia: BOE-A-2011-9280

[. . .]

TÍTULO IV

Control de la actividad

[. . .]

CAPÍTULO II

Participantes

Artículo 15. *Derechos y obligaciones de los participantes en los juegos.*

1. Los participantes en los juegos tienen los siguientes derechos:

a) A obtener información clara y veraz sobre las reglas del juego en el que deseen participar.

b) A cobrar los premios que les pudieran corresponder en el tiempo y forma establecidos, de conformidad con la normativa específica de cada juego.

c) A formular ante la Comisión Nacional del Juego las reclamaciones contra las decisiones del operador que afecten a sus intereses.

d) Al tiempo de uso correspondiente al precio de la partida de que se trate.

e) A jugar libremente, sin coacciones o amenazas provenientes de otros jugadores o de cualquier otra tercera persona.

f) A conocer en cualquier momento el importe que ha jugado o apostado, así como en el caso de disponer de una cuenta de usuario abierta en el operador de juego, a conocer el saldo de la misma.

g) A identificarse de modo seguro mediante el documento nacional de identidad, pasaporte o documento equivalente o mediante sistema de firma electrónica reconocida, así como a la protección de sus datos personales conforme a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

h) A conocer en todo momento la identidad del operador de juego, especialmente en el caso de juegos telemáticos, así como a conocer, en el caso de reclamaciones o posibles infracciones, la identidad del personal que interactúe con los participantes.

i) A recibir información sobre la práctica responsable del juego.

2. Los participantes en los juegos tienen las siguientes obligaciones:

a) Identificarse ante los operadores de juego en los términos que reglamentariamente se establezcan.

b) Cumplir las normas y reglas que, en relación con los participantes, se establezcan en las órdenes ministeriales que se aprueben de conformidad con el artículo 5 de esta Ley.

c) No alterar el normal desarrollo de los juegos.

3. La relación entre el participante y el operador habilitado constituye una relación de carácter privado, y por tanto, las disputas o controversias que pudieran surgir entre ellos estarán sujetas a los Juzgados y Tribunales del orden jurisdiccional civil, sin perjuicio del ejercicio de la potestad sancionadora ejercida por la Comisión Nacional del Juego dentro de las competencias reconocidas en esta Ley.

4. Los operadores habilitados establecerán los procedimientos adecuados para mantener la privacidad de los datos de los usuarios de conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa complementaria.

Los operadores únicamente tratarán los datos de los participantes que fueran necesarios para el adecuado desarrollo de la actividad de juego para la que hubieran sido autorizados y para el cumplimiento de las obligaciones establecidas en esta Ley. Los datos serán cancelados una vez cumplidas las finalidades que justificaron su tratamiento.

En todo caso, de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, los operadores deberán informar a los usuarios acerca del tratamiento de sus datos de carácter personal y las finalidades para las que se produce el tratamiento, así como los derechos que les corresponden de conformidad con la normativa vigente en materia de protección de datos de carácter personal.

Los operadores deberán asimismo implantar sobre los ficheros y tratamientos las medidas de seguridad establecidas en la normativa vigente en materia de protección de datos y dar cumplimiento al deber de secreto impuesto por dicha normativa.

CAPÍTULO III

Homologación de los sistemas técnicos de juego

Artículo 16. *Homologación de los sistemas técnicos de juego.*

1. Las entidades que lleven a cabo la organización, explotación y desarrollo de juegos regulados en esta Ley dispondrán del material software, equipos, sistemas, terminales e instrumentos en general necesarios para el desarrollo de estas actividades, debidamente homologados.

2. La homologación de los sistemas técnicos de juego, así como el establecimiento de las especificaciones necesarias para su funcionamiento, corresponde a la Comisión Nacional del Juego, que aprobará en el marco de los criterios fijados por el Ministerio de Economía y Hacienda y el Consejo de Políticas del Juego, el procedimiento de certificación de los sistemas técnicos de juego incluyendo, en su caso, las homologaciones de material de juego. La Comisión Nacional del Juego velará para que el establecimiento de las especificaciones, así como los procedimientos de certificación y homologación de material de juego, no introduzcan obstáculos que pudieren distorsionar injustificadamente la competencia en el mercado.

3. Las homologaciones y certificaciones validadas por los órganos competentes de las Comunidades Autónomas para la concesión de títulos habilitantes de ámbito autonómico, podrán tener efectos en los procedimientos regulados en esta Ley en los términos que reglamentariamente se establezcan.

4. En los procedimientos de homologación de los sistemas técnicos de juego que puedan afectar de manera relevante al tratamiento de datos de carácter personal por parte de los operadores, la Comisión Nacional del Juego solicitará informe a la Agencia Española de Protección de Datos.

[. . .]

TÍTULO V

La Administración del Juego

[. . .]

Artículo 22. *Los Registros del sector del juego.*

1. La Comisión Nacional del Juego constituirá, bajo su dependencia y control, los siguientes Registros de ámbito estatal:

a) El Registro General de Licencias de Juego, en el que se practicarán las inscripciones de carácter provisional de las empresas que participen en los procedimientos concurrenciales de licencias generales, así como las inscripciones de carácter definitivo de las entidades que hayan obtenido una licencia para desarrollar la actividad de juego.

b) El Registro General de Interdicciones de Acceso al Juego, en el que se inscribirá la información necesaria para hacer efectivo el derecho de los ciudadanos a que les sea prohibida la participación en las actividades de juego en los casos en que sea necesaria la identificación para la participación en las mismas. Asimismo, se inscribirá la información relativa a aquellas otras personas que, por resolución judicial tengan prohibido el acceso al juego o se hallen incapacitadas legalmente. Los requisitos de carácter subjetivo preceptivos para la inscripción en este registro serán determinados por la Comisión Nacional del Juego. La información de este registro se facilitará a los operadores de juego con la finalidad de impedir el acceso al juego de las personas inscritas en el mismo.

Reglamentariamente se establecerá el procedimiento para coordinar la comunicación de datos entre los Registros de Interdicción de Acceso al Juego de las distintas Comunidades Autónomas y el Registro General de Interdicciones de Acceso al Juego.

c) Registro de Personas Vinculadas a Operadores de Juego, en el que se inscribirán los datos de los accionistas, partícipes o titulares significativos de la propia empresa de juego, su personal directivo y empleados directamente involucrados en el desarrollo de los juegos, así como sus cónyuges o personas con las que convivan, ascendientes y descendientes en primer grado.

2. El tratamiento de los datos de carácter personal en los ficheros y registros a los que se refiere el apartado anterior, para los fines previstos en esta Ley, no requerirá del consentimiento de sus titulares.

Reglamentariamente se determinará el contenido concreto de los registros a los que se refiere el presente artículo. Los registros no incluirán más datos que los estrictamente necesarios para el cumplimiento de las finalidades previstas para los mismos en esta Ley.

El contenido de los registros referidos en el presente artículo no presenta carácter público, quedando limitada la comunicación de los datos contenidos en los mismos, única y exclusivamente, a las finalidades previstas en esta Ley.

3. Reglamentariamente se establecerá la organización y funcionamiento de los registros del sector del juego. En este marco, la Comisión Nacional del Juego y los órganos competentes de las Comunidades Autónomas podrán acordar, mediante los oportunos convenios de colaboración, la interconexión de sus registros de juego y el intercambio de datos e información tributaria, con pleno respeto a la normativa reguladora de la protección de datos de carácter personal.

[. . .]

Artículo 24. *Inspección y Control.*

1. Al objeto de garantizar lo dispuesto en esta Ley y en las disposiciones que la complementen, corresponderá a la Comisión Nacional del Juego la auditoría, vigilancia, inspección y control de todos los aspectos y estándares administrativos, económicos, procedimentales, técnicos, informáticos, telemáticos y de documentación, relativos al desarrollo de las actividades previstas en esta Ley.

Asimismo, corresponderá a la Comisión Nacional del Juego la investigación y persecución de los juegos ilegales, sin perjuicio de las facultades que correspondan a las Fuerzas y Cuerpos de Seguridad competentes y al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias en los términos del artículo 45.4 f) de la Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y de la financiación del terrorismo. La Comisión Nacional del Juego establecerá los procedimientos necesarios en orden al cumplimiento de las funciones antes citadas.

Las Fuerzas y Cuerpos de Seguridad del Estado, de acuerdo con lo establecido en el artículo 12.1.A), letra d), de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, colaborarán con la Comisión Nacional del Juego en las funciones de vigilancia e inspección del cumplimiento de la normativa en materia de juego. Si como resultado de la actividad inspectora llevada a cabo por las Fuerzas y Cuerpos de Seguridad del Estado en el ejercicio de las funciones de colaboración con la Comisión Nacional del Juego se comprobara la existencia de indicios de la comisión de una infracción, se levantará la oportuna acta que será enviada a los órganos competentes para iniciar el procedimiento sancionador.

2. Por la Comisión Nacional del Juego se establecerán los procedimientos adicionales para el seguimiento y control de los operadores que realicen actividades de juego sujetas a reserva en virtud de una ley y del cumplimiento de las condiciones que se establezcan a los mismos, en especial, en relación con la protección del orden público y la prevención del blanqueo de capitales y financiación del terrorismo. En el supuesto de que, en el ejercicio de su labor inspectora, la Comisión Nacional del Juego apreciara posibles infracciones de las obligaciones establecidas en la Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y de la financiación del terrorismo, informará a la Secretaría de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias en los términos del artículo 48.1 de la citada Ley.

3. La Comisión Nacional del Juego podrá efectuar un control sobre la cuenta de usuario del participante en las actividades de juego objeto de esta Ley, así como de los operadores o proveedores de servicios de juego. La Comisión Nacional del Juego tendrá acceso a los datos de carácter personal recogidos en la cuenta de usuario de los participantes, respetando en todo momento lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos y su normativa de desarrollo.

Las Administraciones Públicas darán acceso a la Comisión Nacional del Juego a sus bases de datos con la finalidad de comprobar la identidad del participante y, especialmente, su condición de mayor de edad.

4. Los operadores habilitados, sus representantes legales y el personal que en su caso se encuentre al frente de las actividades en el momento de la inspección, tendrán la obligación de facilitar a los inspectores y a su personal auxiliar el acceso a los locales y a sus diversas dependencias, así como el examen de los soportes técnicos e informáticos, libros, registros y documentos que solicite la inspección. El resultado de la inspección se hará constar en acta que tendrá la naturaleza de documento público y hará prueba, salvo que se acredite lo contrario, de los hechos y circunstancias que la motiven.

El acta deberá ser firmada por el funcionario que la extienda y por la persona o representante de la entidad fiscalizada, quien podrá hacer constar cuantas observaciones estime convenientes. Se entregará copia del acta a la persona o representante de la entidad fiscalizada, dejando constancia, en su caso, de su negativa a firmarla o a estar presente en el desarrollo de la inspección.

En el ejercicio de las funciones de inspección el personal de la Comisión Nacional del Juego tendrá la condición de autoridad. El ejercicio de las facultades de inspección y control podrá ser objeto de convenio con las Comunidades Autónomas respecto de las actividades y

de los medios o instrumentos situados en su territorio, con excepción de las de carácter resolutorio.

La Comisión Nacional del Juego colaborará con otros organismos reguladores del Espacio Económico Europeo en la persecución del juego ilegal, mediante la adopción de medidas coordinadas para obtener la cesación en la prestación de servicios ilegales de juego y el intercambio de información.

5. La Comisión Nacional del Juego podrá firmar acuerdos de corregulación que coadyuven al cumplimiento de las obligaciones establecidas en esta Ley, en particular en lo referido a la publicidad, en los términos que se determinen reglamentariamente. En la medida en que dichos acuerdos afecten a la publicidad efectuada por los prestadores del servicio de comunicación audiovisual, deberá recabarse informe del Consejo Estatal de Medios Audiovisuales con carácter previo a la firma de los mismos. Los sistemas de autorregulación se dotarán de órganos independientes de control para asegurar el cumplimiento eficaz de los compromisos asumidos por las empresas adheridas. Sus códigos de conducta podrán incluir, entre otras, medidas individuales o colectivas de autocontrol previo de los contenidos publicitarios y deberán establecer sistemas eficaces de resolución extrajudicial de reclamaciones que cumplan los requisitos establecidos en la normativa comunitaria y, como tales, sean notificados a la Comisión Europea, de conformidad con lo previsto en la Resolución del Consejo de 25 de mayo de 2000 relativo a la red comunitaria de órganos nacionales de solución extrajudicial de litigios en materia de consumo o cualquier disposición equivalente.

[. . .]

§ 47

Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 318, de 31 de diciembre de 2010
Última modificación: 2 de noviembre de 2013
Referencia: BOE-A-2010-20139

[. . .]

TÍTULO II

Derechos de los usuarios de los servicios postales

[. . .]

Artículo 7. *Protección de datos.*

1. Conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, los operadores que presten servicios postales no podrían facilitar ningún dato relativo a la existencia del envío postal, a su clase, a sus circunstancias exteriores, a la identidad del remitente y del destinatario, ni a sus direcciones.

2. La obligación de protección de los datos incluirá el deber de secreto de los de carácter personal, la confidencialidad de la información transmitida o almacenada y la protección de la intimidad.

[. . .]

TÍTULO V

Acceso a la red postal de los operadores y resolución de conflictos entre ellos

CAPÍTULO I

Acceso a la red postal y a otras infraestructuras postales

[. . .]

Artículo 47. *Acceso a otras infraestructuras.*

Reglamentariamente se determinarán las condiciones de acceso de los titulares de autorizaciones administrativas singulares de manera transparente y no discriminatoria a otras infraestructuras postales tales como son el sistema de código postal, la base de datos de direcciones, los apartados postales, los buzones de distribución, la información sobre cambios de dirección, el servicio de reexpedición o el servicio de devolución al remitente, siempre que ello resulte necesario para proteger el interés de los usuarios o favorecer una competencia real, según modalidades técnicas y tarifarias previstas en los acuerdos firmados a este fin con el operador designado, todo ello sin perjuicio de lo dispuesto en la normativa sobre protección de datos.

La Comisión Nacional del Sector Postal velará por la observancia de los principios de transparencia y no discriminación en dicho acceso.

[. . .]

Artículo 62. *Sanciones.*

1. Las infracciones leves se sancionarán con multa de 200 a 8.000 euros, las graves con multa de 8.001 a 80.000 euros y las muy graves con multa de 80.001 a 400.000 euros.

2. Las infracciones muy graves, en atención a las circunstancias que concurran en su comisión, podrán dar lugar a la revocación de la autorización administrativa singular para la prestación del servicio por el infractor. Asimismo podrán llevar aparejado el precintado, la incautación de los equipos o vehículos o la clausura de las instalaciones, hasta tanto no se disponga de la oportuna autorización administrativa.

3. La sanción firme por la infracción tipificada en el artículo 59.e) llevará aparejada, desde que se produzca, la inhabilitación del infractor para el ejercicio de la actividad postal por el plazo de un año.

4. Las cuantías señaladas en este artículo podrán ser actualizadas por la ley de presupuestos generales del Estado.

5. El importe de la sanción firme impuesta al operador postal, de acuerdo con la legislación de protección de datos de carácter personal por hechos que sean a su vez constitutivos de infracción postal, se descontará de la sanción de esta naturaleza que corresponda, con el límite del 50 por ciento de ella.

[. . .]

Disposición final segunda. *Puesta en funcionamiento del censo promocional.*

La Comisión Nacional del Sector Postal, en colaboración con los organismos competentes, en el plazo de un año desde la entrada en vigor de la presente ley, adoptará las medidas necesarias para garantizar el efectivo funcionamiento del censo promocional a que se refiere el artículo 31 de la Ley Orgánica de Protección de Datos.

[. . .]

§ 48

Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 103, de 29 de abril de 2010
Última modificación: 4 de septiembre de 2018
Referencia: BOE-A-2010-6737

[. . .]

CAPÍTULO II

De la diligencia debida

[. . .]

Sección 3.ª Medidas reforzadas de diligencia debida

[. . .]

Artículo 15. *Tratamiento de datos de personas con responsabilidad pública.*

1. A fin de dar cumplimiento a las medidas establecidas en el artículo anterior, los sujetos obligados podrán proceder a la creación de ficheros donde se contengan los datos identificativos de las personas con responsabilidad pública, aun cuando no mantuvieran con las mismas una relación de negocios.

A tal efecto los sujetos obligados podrán recabar la información disponible acerca de las personas con responsabilidad pública sin contar con el consentimiento del interesado, aun cuando dicha información no se encuentre disponible en fuentes accesibles al público.

Los datos contenidos en los ficheros creados por los sujetos obligados únicamente podrán ser utilizados para el cumplimiento de las medidas reforzadas de diligencia debida previstas en esta Ley.

2. Será igualmente posible la creación por terceros distintos de los sujetos obligados de ficheros en los que se incluyan los datos identificativos de quienes tengan la condición de personas con responsabilidad pública con la exclusiva finalidad de colaborar con los sujetos obligados en el cumplimiento de las medidas reforzadas de diligencia debida.

Quienes procedan a la creación de estos ficheros no podrán emplear los datos para ninguna otra finalidad distinta de la señalada en el párrafo anterior.

3. El tratamiento y cesión de los datos a los que se refieren los dos apartados anteriores quedará sujeto a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

No obstante, no será preciso informar a los afectados acerca de la inclusión de sus datos en los ficheros a los que se refiere este artículo.

4. Los sujetos obligados y los terceros a que se refiere el apartado 2 deberán establecer procedimientos que permitan la actualización continua de los datos contenidos en los ficheros relativos a las personas con responsabilidad pública.

En todo caso deberán implantarse sobre el fichero las medidas de seguridad de nivel alto previstas en la normativa de protección de datos de carácter personal.

[. . .]

CAPÍTULO III

De las obligaciones de información

[. . .]

Artículo 24. *Prohibición de revelación.*

1. Los sujetos obligados y sus directivos o empleados no revelarán al cliente ni a terceros que se ha comunicado información al Servicio Ejecutivo de la Comisión, o que se está examinando o puede examinarse alguna operación por si pudiera estar relacionada con el blanqueo de capitales o con la financiación del terrorismo.

Esta prohibición no incluirá la revelación a las autoridades competentes, incluidos los órganos centralizados de prevención, o la revelación por motivos policiales en el marco de una investigación penal.

2. La prohibición establecida en el apartado precedente no impedirá:

a) La comunicación de información entre entidades financieras pertenecientes al mismo grupo. A estos efectos, se estará a la definición de grupo establecida en el artículo 42 del Código de Comercio.

b) La comunicación de información entre los sujetos obligados a que se refieren los párrafos m) y ñ) del artículo 2.1, cuando ejerzan sus actividades profesionales, ya sea como empleados o de otro modo, dentro de la misma entidad jurídica o en una red. Se entenderá por red, a estos efectos, la estructura más amplia a la que pertenece la persona y que comparte una propiedad, gestión o supervisión de cumplimiento comunes.

c) La comunicación de información, referida a un mismo cliente y a una misma operación en la que intervengan dos o más entidades o personas, entre entidades financieras o entre los sujetos obligados a que se refieren los párrafos m) y ñ) del artículo 2.1, siempre que pertenezcan a la misma categoría profesional y estén sujetos a obligaciones equivalentes en lo relativo al secreto profesional y a la protección de datos personales. La información intercambiada se utilizará exclusivamente a efectos de la prevención del blanqueo de capitales y de la financiación del terrorismo.

Las excepciones establecidas en las letras anteriores también serán aplicables a la comunicación de información entre personas o entidades domiciliadas en la Unión Europea o en países terceros equivalentes.

Queda prohibida la comunicación de información con personas o entidades domiciliadas en países terceros no calificados como equivalentes o respecto de los que la Comisión Europea adopte la decisión a que se refiere la Disposición adicional de esta Ley.

3. Cuando los sujetos obligados a que se refieren las letras m) y ñ) del artículo 2.1 intenten disuadir a un cliente de una actividad ilegal, ello no constituirá revelación a efectos de lo dispuesto en el apartado primero.

[. . .]

CAPÍTULO IV

Del control interno

[. . .]

Artículo 26 bis. *Procedimientos internos de comunicación de potenciales incumplimientos.*

1. Los sujetos obligados establecerán procedimientos internos para que sus empleados, directivos o agentes puedan comunicar, incluso anónimamente, información relevante sobre posibles incumplimientos de esta ley, su normativa de desarrollo o las políticas y procedimientos implantados para darles cumplimiento, cometidos en el seno del sujeto obligado.

Estos procedimientos podrán integrarse en los sistemas que hubiera podido establecer el sujeto obligado para la comunicación de informaciones relativas a la comisión de actos o conductas que pudieran resultar contrarios a la restante normativa general o sectorial que les fuere aplicable.

2. Será de aplicación a estos sistemas y procedimientos lo dispuesto en la normativa de protección de datos de carácter personal para los sistemas de información de denuncias internas.

A estos efectos, se considerarán como órganos de control interno y cumplimiento exclusivamente los regulados en el artículo 26 ter.

3. Los sujetos obligados adoptarán medidas para garantizar que los empleados, directivos o agentes que informen de las infracciones cometidas en la entidad sean protegidos frente a represalias, discriminaciones y cualquier otro tipo de trato injusto.

4. La obligación de establecimiento del procedimiento de comunicación descrito en los apartados anteriores, no sustituye la necesaria existencia de mecanismos específicos e independientes de comunicación interna de operaciones sospechosas de estar vinculadas con el blanqueo de capitales o la financiación del terrorismo por parte de empleados a las que se refiere el artículo 18.

5. Reglamentariamente podrán determinarse los sujetos obligados exceptuados del cumplimiento de la obligación prevista en este artículo.

Artículo 26 ter. *Órgano de control interno y representante ante el Servicio Ejecutivo.*

1. Los sujetos obligados designarán como representante ante el Servicio Ejecutivo de la Comisión a una persona residente en España que ejerza cargo de administración o dirección de la sociedad.

En los grupos que integren varios sujetos obligados, el representante será único y deberá ejercer cargo de administración o dirección de la sociedad dominante del grupo.

En el caso de empresarios o profesionales individuales será representante ante el Servicio Ejecutivo de la Comisión el titular de la actividad.

2. Con las excepciones que se determinen reglamentariamente, la propuesta de nombramiento del representante, acompañada de una descripción detallada de su trayectoria profesional, será comunicada al Servicio Ejecutivo de la Comisión que, de forma razonada, podrá formular reparos u observaciones.

El representante ante el Servicio Ejecutivo de la Comisión será responsable del cumplimiento de las obligaciones de información establecidas en la presente ley, para lo que tendrá acceso sin limitación alguna a cualquier información obrante en el sujeto obligado así como en cualquiera de las entidades del grupo, en su caso.

3. Los sujetos obligados cuya administración central se encuentre en otro Estado miembro de la Unión Europea y que operen en España mediante agentes u otras formas de establecimiento permanente distintas de la sucursal deberán nombrar un representante residente en España, que tendrá la consideración de punto central de contacto.

Los sujetos obligados que operen en España en régimen de libre prestación de servicios deberán asimismo designar un representante ante el Servicio Ejecutivo de la Comisión, sin que sea exigible su residencia en España.

4. Los sujetos obligados establecerán un órgano adecuado de control interno responsable de la aplicación de las políticas y procedimientos a que se refiere el artículo 26.

El órgano de control interno, que contará, en su caso, con representación de las distintas áreas de negocio del sujeto obligado, se reunirá, levantando acta expresa de los acuerdos adoptados, con la periodicidad que se determine en el procedimiento de control interno.

5. Para el ejercicio de sus funciones el representante ante el Servicio Ejecutivo de la Comisión y el órgano de control interno deberán contar con los recursos materiales, humanos y técnicos necesarios.

6. Los órganos de prevención del blanqueo de capitales y la financiación del terrorismo operarán, en todo caso, con separación funcional del departamento o unidad de auditoría interna del sujeto obligado.

7. Reglamentariamente se determinarán las categorías de sujetos obligados que puedan exceptuarse de la obligación de constitución de un órgano de control interno, siendo las funciones de éste ejercidas en tales supuestos por el representante ante el Servicio Ejecutivo de la Comisión.

La norma reglamentaria determinará también las categorías de sujetos obligados para los que sea exigible la constitución de unidades técnicas para el tratamiento y análisis de la información.

[. . .]

Artículo 32. *Protección de datos de carácter personal.*

1. El tratamiento de datos de carácter personal, así como los ficheros, automatizados o no, creados para el cumplimiento de las disposiciones de esta Ley se someterán a lo dispuesto en la Ley Orgánica 15/1999 y su normativa de desarrollo.

2. No se requerirá el consentimiento del interesado para el tratamiento de datos que resulte necesario para el cumplimiento de las obligaciones de información a que se refiere el Capítulo III.

Tampoco será necesario el mencionado consentimiento para las comunicaciones de datos previstas en el citado Capítulo y, en particular, para las previstas en el artículo 24.2.

3. En virtud de lo dispuesto en el artículo 24.1, y en relación con las obligaciones a las que se refiere el apartado anterior, no será de aplicación al tratamiento de datos la obligación de información prevista en el artículo 5 de la Ley Orgánica 15/1999.

Asimismo, no serán de aplicación a los ficheros y tratamientos a los que se refiere este precepto las normas contenidas en la citada Ley Orgánica referidas al ejercicio de los derechos de acceso, rectificación, cancelación y oposición. En caso de ejercicio de los citados derechos por el interesado, los sujetos obligados se limitarán a ponerle de manifiesto lo dispuesto en este artículo.

Lo dispuesto en el presente apartado será igualmente aplicable a los ficheros creados y gestionados por el Servicio Ejecutivo de la Comisión para el cumplimiento de las funciones que le otorga esta Ley.

4. Los órganos centralizados de prevención a los que se refiere el artículo 27 tendrán la condición de encargados del tratamiento a los efectos previstos en la normativa de protección de datos de carácter personal.

5. Serán de aplicación a los ficheros a los que se refiere este artículo las medidas de seguridad de nivel alto previstas en la normativa de protección de datos de carácter personal.

Artículo 33. *Intercambio de información entre sujetos obligados y ficheros centralizados de prevención del fraude.*

1. Sin perjuicio de lo establecido en el artículo 24.2, cuando concurran las circunstancias excepcionales que se determinen reglamentariamente, la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias podrá acordar el intercambio de información referida a determinado tipo de operaciones distintas de las previstas en el artículo 18 o a clientes sujetos a determinadas circunstancias siempre que el mismo se

produzca entre sujetos obligados que se encuentren en una o varias de las categorías previstas en el artículo 2.

El Acuerdo determinará en todo caso el tipo de operación o la categoría de cliente respecto de la que se autoriza el intercambio de información, así como las categorías de sujetos obligados que podrán intercambiar la información.

2. Asimismo, los sujetos obligados podrán intercambiar información relativa a las operaciones a las que se refieren los artículos 18 y 19 con la única finalidad de prevenir o impedir operaciones relacionadas con el blanqueo de capitales o la financiación del terrorismo cuando de las características u operativa del supuesto concreto se desprenda la posibilidad de que, una vez rechazada, pueda intentarse ante otros sujetos obligados el desarrollo de una operativa total o parcialmente similar a aquélla.

3. Los sujetos obligados y las autoridades judiciales, policiales y administrativas competentes en materia de prevención o represión del blanqueo de capitales o de la financiación del terrorismo podrán consultar la información contenida en los ficheros que fueren creados, de acuerdo con lo previsto en la normativa vigente en materia de protección de datos de carácter personal, por entidades privadas con la finalidad de prevención del fraude en el sistema financiero, siempre que el acceso a dicha información fuere necesario para las finalidades descritas en los apartados anteriores.

4. El acceso a los datos a los que se refiere este precepto deberá quedar limitado a los órganos de control interno previstos en el artículo 26 ter, con inclusión de las unidades técnicas que constituyan los sujetos obligados.

5. No será de aplicación a los intercambios de información previstos en este artículo lo dispuesto en la Ley Orgánica 15/1999 en lo referente a la exigencia de consentimiento del interesado, el deber de información al mismo y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Serán de aplicación a los tratamientos derivados de las comunicaciones previstas en este artículo las medidas de seguridad de nivel alto previstas en la normativa de protección de datos de carácter personal.

[. . .]

CAPÍTULO VI

Otras disposiciones

[. . .]

Artículo 43. *Fichero de Titularidades Financieras.*

1. Con la finalidad de prevenir e impedir el blanqueo de capitales y la financiación del terrorismo, las entidades de crédito deberán declarar al Servicio Ejecutivo de la Comisión, con la periodicidad que reglamentariamente se determine, la apertura o cancelación de cuentas corrientes, cuentas de ahorro, cuentas de valores y depósitos a plazo.

La declaración contendrá, en todo caso, los datos identificativos de los titulares, representantes o autorizados, así como de cualesquiera otras personas con poderes de disposición, la fecha de apertura o cancelación, el tipo de cuenta o depósito y los datos identificativos de la entidad de crédito declarante.

2. Los datos declarados serán incluidos en un fichero de titularidad pública, denominado Fichero de Titularidades Financieras, del cual será responsable la Secretaría de Estado de Economía.

El Servicio Ejecutivo de la Comisión, como encargado del tratamiento, determinará, con arreglo a lo establecido en la Ley Orgánica 15/1999, las características técnicas del fichero, pudiendo aprobar las instrucciones pertinentes.

3. Con ocasión de la investigación de delitos relacionados con el blanqueo de capitales o la financiación del terrorismo, los jueces de instrucción, el Ministerio Fiscal y, previa autorización judicial o del Ministerio Fiscal, las Fuerzas y Cuerpos de Seguridad, podrán obtener los datos declarados en el Fichero de Titularidades Financieras. El Servicio Ejecutivo

de la Comisión podrá obtener los referidos datos para el ejercicio de sus competencias. La Agencia Estatal de Administración Tributaria podrá obtener los referidos datos en los términos previstos en la Ley 58/2003, de 17 de diciembre, General Tributaria.

Toda petición de acceso a los datos del Fichero de Titularidades Financieras habrá de ser adecuadamente motivada por el órgano requirente, que será responsable de la regularidad del requerimiento. En ningún caso podrá requerirse el acceso al Fichero para finalidades distintas de la prevención o represión del blanqueo de capitales o de la financiación del terrorismo.

4. Sin perjuicio de las competencias que correspondan a la Agencia Española de Protección de Datos, un miembro del Ministerio Fiscal designado por el Fiscal General del Estado de conformidad con los trámites previstos en el Estatuto Orgánico del Ministerio Fiscal y que durante el ejercicio de esta actividad no se encuentre desarrollando su función en alguno de los órganos del Ministerio Fiscal encargados de la persecución de los delitos de blanqueo de capitales o financiación del terrorismo velará por el uso adecuado del fichero, a cuyos efectos podrá requerir justificación completa de los motivos de cualquier acceso.

[. . .]

Artículo 48 bis. *Cooperación internacional.*

1. La Secretaría de la Comisión, el Servicio Ejecutivo de la Comisión o los órganos supervisores a que se refiere el artículo 44, cooperarán por propia iniciativa o previa solicitud, con otras autoridades competentes de la Unión Europea siempre que sea necesario para llevar a cabo las funciones establecidas en esta ley, haciendo uso, a tal fin, de todas las facultades que la misma les atribuye. En el marco de esta cooperación se facilitará a las Autoridades Europeas de Supervisión la información necesaria para permitirles llevar a cabo sus obligaciones en materia de prevención del blanqueo de capitales y de la financiación del terrorismo.

2. En el caso de autoridades competentes de terceros países no miembros de la Unión Europea, la cooperación e intercambio de información se condicionará a lo dispuesto en los Convenios y Tratados Internacionales o, en su caso, al principio general de reciprocidad, así como al sometimiento de dichas autoridades extranjeras a las mismas obligaciones de secreto profesional que rigen para las españolas.

3. El intercambio de información del Servicio Ejecutivo de la Comisión con Unidades de Inteligencia Financiera de Estados de la Unión Europea se realizará de conformidad con lo dispuesto en los artículos 51 a 57 de la Directiva 2015/849, del Parlamento Europeo y del Consejo, de 20 de mayo de 2015 relativa a la prevención de la utilización del sistema financiero para la prevención del blanqueo de capitales o la financiación del terrorismo.

4. El intercambio de información del Servicio Ejecutivo de la Comisión con Unidades de Inteligencia Financiera de terceros países no miembros de la Unión Europea se realizará de acuerdo con los principios del Grupo Egmont o en los términos del correspondiente memorando de entendimiento. Los memorandos de entendimiento con Unidades de Inteligencia Financiera serán suscritos por el Director del Servicio Ejecutivo, previa autorización de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, debiendo contar con el previo informe favorable de la Agencia Española de Protección de Datos.

5. La Secretaría de la Comisión, el Servicio Ejecutivo de la Comisión o los órganos supervisores a que se refiere el artículo 44 podrán utilizar la información recibida únicamente para los fines para los que las autoridades cedentes hayan dado su consentimiento. Esta información no será transmitida a otros organismos o personas físicas y jurídicas sin el consentimiento expreso de las autoridades competentes que la hayan divulgado.

6. A requerimiento de la Unidad de Inteligencia Financiera de otro Estado miembro de la Unión Europea, el Servicio Ejecutivo de la Comisión estará facultado para suspender una transacción en curso, cuando concurran indicios de blanqueo de capitales o financiación del terrorismo a fin de que por parte de la Unidad de Inteligencia Financiera requirente se proceda a analizar la transacción, confirmar la sospecha y comunicar los resultados del

análisis a las autoridades competentes. En los casos de suspensión por indicios de financiación de terrorismo, informará a la Secretaría de la Comisión de Vigilancia de Actividades de Financiación del Terrorismo cuando exista la previa autorización de la Unidad de Inteligencia Financiera requirente.

La suspensión se acordará bajo la responsabilidad de la Unidad de Inteligencia Financiera requirente y será efectiva por un periodo máximo de un mes. Transcurrido dicho plazo, cesará la suspensión salvo que fuera ratificada o prorrogada judicialmente a solicitud del Ministerio Fiscal.

[. . .]

Artículo 63. *Comunicación de infracciones.*

1. Los empleados, directivos y agentes de los sujetos obligados que conozcan hechos o situaciones que puedan ser constitutivos de infracciones contempladas en esta ley, los podrán poner en conocimiento del Servicio Ejecutivo de la Comisión.

2. Las comunicaciones serán remitidas al Servicio Ejecutivo de la Comisión por escrito e incorporarán todos los documentos e informaciones sobre los hechos denunciados que permitan justificar la denuncia. Mediante orden del Ministro de Economía y Empresa se aprobará el modelo de comunicación y se establecerán las características y requisitos del canal de recepción de comunicaciones, a fin de asegurar su confidencialidad y seguridad.

3. Los programas de formación de las entidades deberán incluir la información sobre la existencia de estos mecanismos.

Artículo 64. *Tratamiento de las comunicaciones.*

1. El Servicio Ejecutivo de la Comisión determinará si existe o no sospecha fundada de infracción en las comunicaciones recibidas de conformidad con el artículo 63. De no existir sospecha fundada o cuando no se concreten suficientemente los hechos o personas responsables de la infracción, requerirá a la persona comunicante para que aclare el contenido de la comunicación realizada, o lo complemente con nueva información, concediendo un plazo para ello no inferior a 15 días. Transcurrido el plazo fijado para la aclaración o aportación de nueva información, sin que pueda determinarse sospecha fundada, se procederá al archivo de la comunicación.

2. Las comunicaciones recibidas no tendrán valor probatorio y no podrán ser incorporadas directamente al procedimiento administrativo. Si existen indicios suficientes de veracidad en los hechos imputados y éstos son desconocidos para la Administración, el Servicio Ejecutivo de la Comisión, o los supervisores de las entidades financieras, en caso de convenio de los previstos en el artículo 44. 2 m) de la ley, podrán:

a) Utilizar la información obtenida para la definición del nuevo plan de inspección.

b) Realizar actuaciones adicionales de inspección, que podrán llevarse a cabo de manera independiente o incardinarse en las acciones de supervisión planificadas en el contexto del desarrollo del plan anual de inspección aprobado.

3. Los resultados de las actuaciones de inspección llevadas a cabo por el Servicio Ejecutivo de la Comisión serán remitidas a la Secretaría de la Comisión, que las elevará a la consideración del Comité Permanente. Cuando las actuaciones de comprobación pongan de manifiesto la posible existencia de un ilícito penal, la información será remitida al Ministerio Fiscal para su investigación.

Artículo 65. *Protección de las personas.*

1. Las comunicaciones realizadas al amparo del artículo 63:

a) no constituirán violación o incumplimiento de las restricciones sobre divulgación de información impuestas por vía contractual o por cualquier disposición legal, reglamentaria o administrativa que pudieran afectar a la persona comunicante, a las personas estrechamente vinculadas con ésta, a las sociedades que administre o de las que sea titular real;

b) no constituirán infracción de ningún tipo en el ámbito de la normativa laboral por parte de la persona comunicante, ni de ella podrá derivar trato injusto o discriminatorio por parte del empleador;

c) no generarán ningún derecho de compensación o indemnización a favor de la empresa a la que presta servicios la persona comunicante o de un tercero.

2. El Servicio Ejecutivo de la Comisión informará de los diferentes mecanismos legales que la normativa en vigor habilita para la garantía de estos derechos.

3. Las comunicaciones tendrán carácter confidencial, no pudiendo desvelar el Servicio Ejecutivo de la Comisión los datos identificativos de las personas que las hubieran realizado. En el caso de que, como consecuencia de la comunicación realizada, se inicie un expediente sancionador contra una persona física o jurídica, no se incluirán en ningún caso los datos de la persona que llevó a cabo la comunicación.

4. La comunicación realizada al amparo de lo previsto en el artículo 63 no conferirá por sí sola la condición de interesado en el procedimiento administrativo que pudiera iniciarse contra el infractor.

[...]

§ 49

Ley Orgánica 2/2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 55, de 4 de marzo de 2010
Última modificación: 22 de septiembre de 2015
Referencia: BOE-A-2010-3514

[. . .]

TÍTULO II

De la interrupción voluntaria del embarazo

[. . .]

CAPÍTULO II

Garantías en el acceso a la prestación

[. . .]

Artículo 20. *Protección de la intimidad y confidencialidad.*

1. Los centros que presten la interrupción voluntaria del embarazo asegurarán la intimidad de las mujeres y la confidencialidad en el tratamiento de sus datos de carácter personal.

2. Los centros prestadores del servicio deberán contar con sistemas de custodia activa y diligente de las historias clínicas de las pacientes e implantar en el tratamiento de los datos las medidas de seguridad de nivel alto previstas en la normativa vigente de protección de datos de carácter personal.

Artículo 21. *Tratamiento de datos.*

1. En el momento de la solicitud de información sobre la interrupción voluntaria del embarazo, los centros, sin proceder al tratamiento de dato alguno, habrán de informar a la solicitante que los datos identificativos de las pacientes a las que efectivamente se les realice la prestación serán objeto de codificación y separados de los datos de carácter clínico asistencial relacionados con la interrupción voluntaria del embarazo.

2. Los centros que presten la interrupción voluntaria del embarazo establecerán mecanismos apropiados de automatización y codificación de los datos de identificación de las pacientes atendidas, en los términos previstos en esta Ley.

A los efectos previstos en el párrafo anterior, se considerarán datos identificativos de la paciente su nombre, apellidos, domicilio, número de teléfono, dirección de correo electrónico, documento nacional de identidad o documento identificativo equivalente, así como cualquier dato que revele su identidad física o genética.

3. En el momento de la primera recogida de datos de la paciente, se le asignará un código que será utilizado para identificarla en todo el proceso.

4. Los centros sustituirán los datos identificativos de la paciente por el código asignado en cualquier información contenida en la historia clínica que guarde relación con la práctica de la interrupción voluntaria del embarazo, de forma que no pueda producirse con carácter general, el acceso a dicha información.

5. Las informaciones relacionadas con la interrupción voluntaria del embarazo deberán ser conservadas en la historia clínica de tal forma que su mera visualización no sea posible salvo por el personal que participe en la práctica de la prestación, sin perjuicio de los accesos a los que se refiere el artículo siguiente.

Artículo 22. *Acceso y cesión de datos de carácter personal.*

1. Únicamente será posible el acceso a los datos de la historia clínica asociados a los que identifican a la paciente, sin su consentimiento, en los casos previstos en las disposiciones legales reguladoras de los derechos y obligaciones en materia de documentación clínica.

Cuando el acceso fuera solicitado por otro profesional sanitario a fin de prestar la adecuada asistencia sanitaria de la paciente, aquél se limitará a los datos estricta y exclusivamente necesarios para la adecuada asistencia, quedando constancia de la realización del acceso.

En los demás supuestos amparados por la ley, el acceso se realizará mediante autorización expresa del órgano competente en la que se motivarán de forma detallada las causas que la justifican, quedando en todo caso limitado a los datos estricta y exclusivamente necesarios.

2. El informe de alta, las certificaciones médicas y cualquier otra documentación relacionada con la práctica de la interrupción voluntaria del embarazo que sea necesaria a cualquier efecto, será entregada exclusivamente a la paciente o persona autorizada por ella. Esta documentación respetará el derecho de la paciente a la intimidad y confidencialidad en el tratamiento de los datos de carácter personal recogido en este Capítulo.

3. No será posible el tratamiento de la información por el centro sanitario para actividades de publicidad o prospección comercial. No podrá recabarse el consentimiento de la paciente para el tratamiento de los datos para estas actividades.

Artículo 23. *Cancelación de datos.*

1. Los centros que hayan procedido a una interrupción voluntaria de embarazo deberán cancelar de oficio la totalidad de los datos de la paciente una vez transcurridos cinco años desde la fecha de alta de la intervención. No obstante, la documentación clínica podrá conservarse cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud, en cuyo caso se procederá a la cancelación de todos los datos identificativos de la paciente y del código que se le hubiera asignado como consecuencia de lo dispuesto en los artículos anteriores.

2. Lo dispuesto en el apartado anterior se entenderá sin perjuicio del ejercicio por la paciente de su derecho de cancelación, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[. . .]

§ 50

Ley 54/2007, de 28 de diciembre, de Adopción internacional. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 312, de 29 de diciembre de 2007
Última modificación: 29 de julio de 2015
Referencia: BOE-A-2007-22438

[. . .]

TÍTULO I

Disposiciones generales

[. . .]

CAPÍTULO III

Capacidad y requisitos para la adopción internacional

[. . .]

Artículo 13. *Protección de datos de carácter personal.*

1. El tratamiento y la cesión de datos derivados del cumplimiento de las previsiones de la presente ley se encontrarán sometidos a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Los datos obtenidos por las Entidades Públicas o por los organismos acreditados únicamente podrán ser tratados para las finalidades relacionadas con el desarrollo, en cada caso, de las funciones descritas para cada una de ellas en los artículos 5 y 6.3 de la presente ley.

3. La transferencia internacional de los datos a autoridades extranjeras de adopción únicamente se efectuará en los supuestos expresamente previstos en esta ley y en el Convenio de La Haya, de 29 de mayo de 1993, relativo a la protección del niño y a la cooperación en materia de adopción internacional y demás legislación internacional.

[. . .]

§ 51

Ley Orgánica 11/2007, de 22 de octubre, reguladora de los derechos y deberes de los miembros de la Guardia Civil. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 254, de 23 de octubre de 2007
Última modificación: 29 de julio de 2015
Referencia: BOE-A-2007-18391

[. . .]

TÍTULO II

Del ejercicio de derechos fundamentales y libertades públicas

[. . .]

Artículo 5. *Derecho a la intimidad y a la vida privada.*

1. Los miembros de la Guardia Civil tienen garantizados los derechos a la intimidad, a la inviolabilidad del domicilio y al secreto de las comunicaciones, en los términos establecidos en la Constitución y en el resto del ordenamiento jurídico.

A estos efectos el pabellón que tuviera asignado el Guardia Civil en su unidad se considerará domicilio habitual.

2. El jefe de la unidad, centro u órgano donde el Guardia Civil preste sus servicios podrá autorizar, de forma expresamente motivada, el registro personal o de los efectos y pertenencias que estuvieren en los mismos, cuando lo exija la investigación de un hecho delictivo. El registro se realizará con la asistencia del interesado y en presencia de, al menos, un testigo.

3. Los datos relativos a los miembros de la Guardia Civil estarán sujetos a la legislación sobre protección de datos de carácter personal.

[. . .]

§ 52

Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 242, de 9 de octubre de 2007
Última modificación: sin modificaciones
Referencia: BOE-A-2007-17634

[. . .]

Disposición Adicional Segunda. *Régimen jurídico.*

La presente Ley se inscribe en el marco de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la cual, por su propia naturaleza, resulta de aplicación directa, siendo los preceptos de esta Ley especificidades habilitadas por la citada Ley Orgánica en función de la naturaleza de la base de datos que se regula.

[. . .]

§ 53

Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades

Jefatura del Estado
«BOE» núm. 89, de 13 de abril de 2007
Última modificación: 17 de septiembre de 2014
Referencia: BOE-A-2007-7786

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica.

PREÁMBULO

Desde la promulgación de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, han pasado cinco años. En este período se han detectado algunas deficiencias en su funcionamiento que aconsejan su revisión. Además, otros elementos del entorno han cambiado e inducen también a realizar modificaciones. Entre estos hechos se encuentran los acuerdos en política de educación superior en Europa y el impulso que la Unión Europea pretende dar a la investigación en todos sus países miembros. Estas circunstancias aconsejan la corrección de las deficiencias detectadas y la incorporación de algunos elementos que mejoren la calidad de las universidades españolas.

La Ley apuesta decididamente por la armonización de los sistemas educativos superiores en el marco del espacio europeo de educación superior y asume la necesidad de una profunda reforma en la estructura y organización de las enseñanzas, basada en tres ciclos: Grado, Máster y Doctorado. Se da así respuesta al deseo de la comunidad universitaria de asentar los principios de un espacio común, basado en la movilidad, el reconocimiento de titulaciones y la formación a lo largo de la vida. El nuevo modelo de enseñanzas aporta una manera diferente de entender la universidad y sus relaciones con la sociedad. Se trata de ofrecer una formación de calidad que atienda a los retos y desafíos del conocimiento y dé respuesta a las necesidades de la sociedad.

Así, las reformas están guiadas por la voluntad de potenciar la autonomía de las universidades, a la vez que se aumenta la exigencia de rendir cuentas sobre el cumplimiento de sus funciones. Este principio es impulsado por la Unión Europea apoyando la modernización de las universidades europeas con el fin de convertirlas en agentes activos para la transformación de Europa en una economía plenamente integrada en la sociedad del

conocimiento. La autonomía es la principal característica que las universidades tienen para responder con flexibilidad y rapidez a las cambiantes necesidades.

Entre las medidas que potencian la autonomía de nuestras universidades, principio reconocido en el artículo 27 de la Constitución Española, esta Ley flexibiliza el sistema de elección del Rector o de la Rectora y permite que las propias universidades elijan la opción que consideren más adecuada. Asimismo, se asegura que las decisiones de naturaleza académica de las universidades públicas y privadas se adopten por órganos en los que el personal docente e investigador tengan una representación mayoritaria. Por otra parte, la Ley adopta medidas tendentes a asegurar el equilibrio institucional en el seno de las universidades y a profesionalizar su gestión.

Otro de los ejes de la reforma es potenciar el papel y la responsabilidad de todos los agentes del sistema universitario, articulando mejor la relación entre ellos. Las Comunidades Autónomas son responsables de la política universitaria de acuerdo con lo previsto en la Constitución y en los Estatutos de Autonomía, mientras que al Estado, conforme al artículo 149.1.30.ª, le corresponde establecer las normas básicas para el desarrollo del artículo 27.10 que reconoce la autonomía de las universidades. La articulación de este complejo organizativo de Estado-Comunidades Autónomas y universidades requiere alcanzar una armonía de todos los agentes implicados y una relación clara y fluida entre todos ellos. Es especialmente importante articular las relaciones intergubernamentales, de un lado, y de otro, la coordinación y cooperación en el ámbito académico. Por ello, se crea la Conferencia General de Política Universitaria y se constituye el Consejo de Universidades con funciones de asesoramiento, cooperación y coordinación en el ámbito académico. Además, se configura una regulación más adecuada del proceso de verificación de planes de estudios y más respetuosa con el sistema complejo que en materia universitaria conforman la Administración General del Estado, las Comunidades Autónomas y las universidades.

La selección del profesorado funcionario se modifica incorporando un modelo de acreditación que permita que las universidades seleccionen a su profesorado entre los previamente acreditados. Este sistema incorpora para el conjunto de la comunidad académica un mayor rigor en la acreditación y una mayor flexibilidad para las universidades en la selección de su personal.

En relación con la contratación del profesorado, esta Ley establece, siguiendo las pautas de la Ley Orgánica 6/2001, de 21 de diciembre, una serie de modalidades contractuales específicas del ámbito universitario que, por las características propias del trabajo y por las condiciones de la relación laboral, no pueden subsumirse en las figuras previstas en la legislación laboral general. Esta Ley define con mayor precisión la especificidad de estas modalidades contractuales, bien por la necesidad de completar la formación en el caso de los ayudantes y de los profesores ayudantes doctores, bien por la oportunidad de aportar a la universidad el conocimiento y la experiencia de profesionales del sector productivo –profesores asociados– o de docentes e investigadores de prestigio de otras universidades –profesores visitantes–. Debido a las especiales características de la labor docente e investigadora que realiza la universidad, es necesario establecer para estas modalidades mecanismos de temporalidad que favorezcan el desarrollo del proceso académico y que, por otro lado, partan de la lógica conservación de la fuente de conocimiento y experiencia que aportan estos profesionales a la universidad y que es la característica principal que dota de sentido a figuras como la del profesor asociado o la de profesor visitante.

La Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA) tiene un papel muy importante en el binomio autonomía-rendición de cuentas. Para reforzar su papel dentro del sistema universitario, se autoriza su creación como agencia de acuerdo con la Ley de Agencias Estatales para la mejora de los servicios públicos. Con ello, se facilita la coordinación en los procesos de garantía de calidad y la definición de criterios de evaluación.

La implicación de las universidades en la respuesta a las demandas de la sociedad y el sistema productivo es otro de los ejes sobre los que ha girado la presente reforma. Las universidades deben perseguir una mejor formación de sus graduadas y graduados para que éstos sean capaces de adaptarse tanto a las demandas sociales, como a las demandas del sistema científico y tecnológico. También han de dar adecuada respuesta a las necesidades de formación a lo largo de toda la vida y abrirse a quienes, a cualquier edad, deseen acceder a su oferta cultural o educativa. Las universidades, además de un motor para el avance del

conocimiento, deben ser un motor para el desarrollo social y económico del país. Junto a la investigación básica, la universidad deberá impulsar la transferencia al sector productivo de los resultados de su investigación en coordinación y complementariedad con los demás agentes del sistema de ciencia y tecnología. Una de las medidas para contribuir a este objetivo es el impulso decidido de la vinculación entre la investigación universitaria y el entorno productivo del sistema de ciencia y tecnología a través de la creación de institutos mixtos de investigación, que permitirán una relación directa entre los agentes de dicho sistema. Asimismo, se prevé potenciar los mecanismos de intercambio de personal investigador entre el sistema universitario y el productivo.

Además, esta Ley prevé la elaboración de un estatuto del estudiante universitario y la creación del Consejo de estudiantes universitarios, con el fin de articular la necesaria participación del alumnado en el sistema universitario.

Se introduce también una modificación del título XIII de la Ley Orgánica 6/2001, para adecuarlo a la nueva situación del Espacio Europeo de la Enseñanza Superior.

Otro aspecto novedoso es la inclusión de un título dedicado al deporte y la extensión universitaria, pues se considera que tanto el deporte como otras actividades que se contemplan son un aspecto capital en la formación del alumnado universitario.

Esta Ley no olvida el papel de la universidad como transmisor esencial de valores. El reto de la sociedad actual para alcanzar una sociedad tolerante e igualitaria, en la que se respeten los derechos y libertades fundamentales y de igualdad entre hombres y mujeres, debe alcanzar, sin duda, a la universidad. Esta Ley impulsa la respuesta de las universidades a este reto a través no sólo de la incorporación de tales valores como objetivos propios de la universidad y de la calidad de su actividad, sino mediante el establecimiento de sistemas que permitan alcanzar la paridad en los órganos de representación y una mayor participación de la mujer en los grupos de investigación. Los poderes públicos deben remover los obstáculos que impiden a las mujeres alcanzar una presencia en los órganos de gobierno de las universidades y en el nivel más elevado de la función pública docente e investigadora acorde con el porcentaje que representan entre los licenciados universitarios. Además, esta reforma introduce la creación de programas específicos sobre la igualdad de género, de ayuda a las víctimas del terrorismo y el impulso de políticas activas para garantizar la igualdad de oportunidades a las personas con discapacidad.

La Ley tiene también en cuenta la necesidad de potenciar la proyección internacional del sistema universitario español y la movilidad interuniversitaria, promoviendo la oferta educativa e investigadora de las universidades españolas. A tal fin se prevé la constitución de una fundación del sector público estatal.

La sociedad reclama a la universidad del futuro una activa participación en sus procesos vitales. Por esta razón, la acción de la universidad no debe limitarse a la transmisión del saber; debe generar opinión, demostrar su compromiso con el progreso social y ser un ejemplo para su entorno.

La igualdad entre hombres y mujeres, los valores superiores de nuestra convivencia, el apoyo permanente a las personas con necesidades especiales, el fomento del valor del diálogo, de la paz y de la cooperación entre los pueblos, son valores que la universidad debe cuidar de manera especial.

En definitiva, la reforma pretende ser un paso adelante en la organización del sistema universitario hacia una estructura más abierta y flexible, que sitúe a las universidades españolas en una mejor posición para la cooperación interna y la competencia internacional, a través de la creación, transmisión, desarrollo y crítica del conocimiento científico y tecnológico y de la transferencia de sus beneficios a la sociedad, con el fin de que consigan ser atractivas en un mundo globalizado. Una adecuada generación y gestión del conocimiento por parte de las universidades permitirá contribuir a la consecución de un mayor grado de bienestar de los españoles.

Artículo único. *Modificación de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.*

La Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, se modifica en los siguientes términos:

Uno. El párrafo cuarto del apartado 3 del artículo 5 queda redactado del siguiente modo:

«La infracción de lo previsto en los párrafos anteriores supondrá una modificación de las condiciones esenciales del reconocimiento o de la aprobación de la adscripción y podrá ser causa de su revocación.»

Dos. El apartado 4 del artículo 5 queda redactado del siguiente modo:

«4. Los centros universitarios privados deberán estar integrados en una universidad privada, como centros propios de la misma, o adscritos a una pública o privada.»

Tres. Se añade un nuevo párrafo al apartado 2 del artículo 6 redactado del siguiente modo:

«Los poderes públicos y las universidades, a través de sus estatutos, establecerán mecanismos para que en los procesos de acogida de los diferentes miembros de la comunidad universitaria se favorezca el conocimiento suficiente de las lenguas cooficiales.»

Cuatro. El artículo 7 queda redactado del siguiente modo:

«Artículo 7. *Centros y estructuras.*

Las universidades públicas estarán integradas por Escuelas, Facultades, Departamentos, Institutos Universitarios de Investigación y por aquellos otros centros o estructuras necesarios para el desempeño de sus funciones.»

Cinco. El artículo 8 queda redactado del siguiente modo:

«Artículo 8. *Escuelas y Facultades.*

1. Las escuelas y facultades son los centros encargados de la organización de las enseñanzas y de los procesos académicos, administrativos y de gestión conducentes a la obtención de títulos de grado. Podrán impartir también enseñanzas conducentes a la obtención de otros títulos, así como llevar a cabo aquellas otras funciones que determine la universidad.

2. La creación, modificación y supresión de dichos centros, así como la implantación y supresión de las enseñanzas conducentes a la obtención de títulos universitarios de carácter oficial y validez en todo el territorio nacional, de conformidad con lo dispuesto en el artículo 35, serán acordadas por la Comunidad Autónoma, bien por propia iniciativa, con el acuerdo del Consejo de Gobierno de la universidad, bien por iniciativa de la universidad mediante propuesta del Consejo de Gobierno, en ambos casos con informe previo favorable del Consejo Social.

3. De lo señalado en el apartado anterior será informada la Conferencia General de Política Universitaria.»

Seis. El artículo 9 queda redactado del siguiente modo:

«Artículo 9. *Departamentos.*

1. Los departamentos son las unidades de docencia e investigación encargadas de coordinar las enseñanzas de uno o varios ámbitos del conocimiento en uno o varios centros, de acuerdo con la programación docente de la universidad, de apoyar las actividades e iniciativas docentes e investigadoras del profesorado, y de ejercer aquellas otras funciones que sean determinadas por los estatutos.

2. La creación, modificación y supresión de departamentos corresponde a la universidad, conforme a sus estatutos.»

Siete. El apartado 2 del artículo 10 queda redactado del siguiente modo:

«2. Los Institutos Universitarios de Investigación podrán ser constituidos por una o más universidades, o conjuntamente con otras entidades públicas o privadas

mediante convenios u otras formas de cooperación, de conformidad con los estatutos.

Asimismo, las universidades, conjuntamente con los organismos públicos de investigación, con los centros del Sistema Nacional de Salud y con otros centros de investigación públicos o privados sin ánimo de lucro, promovidos y participados por una administración pública, podrán constituir Institutos Mixtos de Investigación. A estos efectos, y de acuerdo con lo que establezcan los estatutos de las universidades, el personal docente e investigador podrá ser adscrito a los citados Institutos Mixtos de Investigación.»

Ocho. El apartado 4 del artículo 10 queda redactado del siguiente modo:

«4. Mediante convenio, podrán adscribirse a universidades públicas, como institutos universitarios de investigación, instituciones o centros de investigación de carácter público o privado. La aprobación de la adscripción o, en su caso, desadscripción corresponde a la Comunidad Autónoma, bien por propia iniciativa, con acuerdo del Consejo de Gobierno de la universidad y previo informe favorable del Consejo Social, bien por iniciativa de la universidad mediante propuesta del Consejo de Gobierno, con informe previo favorable del Consejo Social.

De lo señalado en el párrafo anterior será informada la Conferencia General de Política Universitaria.»

Nueve. El artículo 11 queda redactado del siguiente modo:

«Artículo 11. *Centros de educación superior adscritos a universidades.*

1. La adscripción mediante convenio a una universidad pública de centros docentes de titularidad pública o privada para impartir estudios conducentes a la obtención de títulos de carácter oficial y validez en todo el territorio nacional requerirá la aprobación de la Comunidad Autónoma, a propuesta del Consejo de Gobierno de la universidad, previo informe favorable de su Consejo Social.

La adscripción mediante convenio a una universidad privada de centros docentes de titularidad privada para impartir estudios conducentes a la obtención de títulos de carácter oficial y validez en todo el territorio nacional requerirá la aprobación de la Comunidad Autónoma, a propuesta de la universidad.

2. Los centros adscritos deberán estar establecidos en el ámbito territorial de la correspondiente Comunidad Autónoma, o contar, asimismo, con la aprobación de aquélla en la que estuvieran ubicados.

3. Los centros adscritos a una universidad se regirán por lo dispuesto en esta Ley, por las normas dictadas por el Estado y las Comunidades Autónomas en el ejercicio de sus competencias, por el convenio de adscripción y por sus propias normas de organización y funcionamiento. El comienzo de las actividades de los centros adscritos será autorizado por la Comunidad Autónoma.

4. El Gobierno, en cumplimiento de lo dispuesto en el artículo 4.3, establecerá los requisitos básicos que deberán cumplir los centros adscritos.

5. De lo señalado en los apartados 1 y 2 será informada la Conferencia General de Política Universitaria.»

Diez. El artículo 13 queda redactado del siguiente modo:

«Artículo 13. *Órganos de gobierno y representación de las universidades públicas.*

Los estatutos de las universidades públicas establecerán, al menos, los siguientes órganos:

a) Colegiados: Consejo Social, Consejo de Gobierno, Claustro Universitario, Juntas de Escuela y Facultad y Consejos de Departamento.

b) Unipersonales: Rector o Rectora, Vicerrectores o Vicerrectoras, Secretario o Secretaria General, Gerente, Decanos o Decanas de Facultades, Directores o Directoras de Escuelas, de Departamentos y de Institutos Universitarios de Investigación.

La elección de los representantes de los distintos sectores de la comunidad universitaria en el Claustro Universitario, en las Juntas de Facultad o Escuela y en los Consejos de Departamento se realizará mediante sufragio universal, libre, igual, directo y secreto, en cada uno de ellos.

Los estatutos establecerán las normas electorales aplicables, las cuales deberán propiciar en los órganos colegiados la presencia equilibrada entre mujeres y hombres.»

Once. El apartado 1 y el primer párrafo del apartado 2 del artículo 14 quedan redactados del siguiente modo:

«1. El Consejo Social es el órgano de participación de la sociedad en la universidad, y debe ejercer como elemento de interrelación entre la sociedad y la universidad.

2. Corresponde al Consejo Social la supervisión de las actividades de carácter económico de la universidad y del rendimiento de sus servicios y promover la colaboración de la sociedad en la financiación de la universidad. A tal fin, aprobará un plan anual de actuaciones destinado a promover las relaciones entre la universidad y su entorno cultural, profesional, económico y social al servicio de la calidad de la actividad universitaria. Los consejos sociales podrán disponer de la oportuna información y asesoramiento de los órganos de evaluación de las Comunidades Autónomas y de la Agencia Nacional de Evaluación de la Calidad y Acreditación.»

Doce. El apartado 3 del artículo 14 queda redactado del siguiente modo:

«3. La Ley de la Comunidad Autónoma regulará la composición y funciones del Consejo Social y la designación de sus miembros de entre personalidades de la vida cultural, profesional, económica, laboral y social, que no podrán ser miembros de la propia comunidad universitaria. Serán, no obstante, miembros del Consejo Social, el Rector, el Secretario General y el Gerente, así como un profesor, un estudiante y un representante del personal de administración y servicios, elegidos por el Consejo de Gobierno de entre sus miembros. El Presidente del Consejo Social será nombrado por la Comunidad Autónoma en la forma que determine la Ley respectiva.»

Trece. El apartado 2 del artículo 15 queda redactado del siguiente modo:

«2. El Consejo de Gobierno estará constituido por el Rector, que lo presidirá, el Secretario General y el Gerente, y por un máximo de 50 miembros. Del mismo formarán parte los Vicerrectores, una representación de la comunidad universitaria, reflejando la composición de los distintos sectores en el Claustro, y una representación de Decanos y Directores, según establezcan los Estatutos. Además, cuando así lo determinen los Estatutos, podrán ser miembros del Consejo de Gobierno hasta un máximo de tres miembros del Consejo Social, no pertenecientes a la propia comunidad universitaria.»

Catorce. El apartado 1 del artículo 16 queda redactado del siguiente modo:

«1. El Claustro Universitario es el máximo órgano de representación de la comunidad universitaria. Estará formado por el Rector, que lo presidirá, el Secretario General y el Gerente, y un máximo de 300 miembros. Le corresponde la elaboración de los estatutos, la elección del Rector, en su caso, y las demás funciones que le atribuye esta Ley.»

Quince. El apartado 2 del artículo 16 queda redactado del siguiente modo:

«2. Cualquiera que fuese la forma de elección, el Claustro podrá convocar, con carácter extraordinario, elecciones a Rector a iniciativa de un tercio de sus componentes y con la aprobación de dos tercios. La aprobación de la iniciativa llevará consigo la disolución del Claustro y el cese del Rector, que continuará en funciones hasta la toma de posesión del nuevo Rector. El procedimiento será establecido por los estatutos. Si la iniciativa no fuese aprobada, ninguno de sus

signatarios podrá participar en la presentación de otra iniciativa de este carácter hasta pasado un año desde su votación.»

Dieciséis. El apartado 3 del artículo 16 queda redactado del siguiente modo:

«3. Los estatutos regularán la composición y duración del mandato del Claustro, en el que estarán representados los distintos sectores de la comunidad universitaria. En todo caso, la mayoría de sus miembros serán profesores doctores con vinculación permanente a la universidad.»

Diecisiete. El artículo 17 queda sin contenido.

Dieciocho. El artículo 18 queda redactado del siguiente modo:

«La Junta de Escuela o Facultad, presidida por el Decano o Director, es el órgano de Gobierno de ésta. La composición y el procedimiento de elección de sus miembros serán determinados por los Estatutos. En todo caso, la mayoría de sus miembros serán profesores con vinculación permanente a la universidad.»

Diecinueve. El apartado 2 del artículo 20 queda redactado del siguiente modo:

«2. El Rector será elegido por el Claustro, o por la comunidad universitaria mediante elección directa y sufragio universal, según indiquen los estatutos de cada universidad, entre funcionarios en activo del Cuerpo de Catedráticos de Universidad que presten servicios en ella. Los estatutos regularán también el procedimiento para su elección, la duración de su mandato y los supuestos de su sustitución en el caso de vacante, ausencia o enfermedad.

En el caso de que la elección del Rector corresponda al Claustro, para ser proclamado Rector será necesario que un candidato o candidata obtenga en primera votación más de la mitad de los votos a candidaturas emitidos válidamente. Si ningún candidato la alcanza, se procederá a una segunda votación a la que sólo podrán concurrir los dos candidatos con mayor número de votos en la primera votación, y será elegido Rector el candidato que obtenga más votos.

El Rector o la Rectora será nombrado por el órgano correspondiente de la Comunidad Autónoma.»

Veinte. El primer párrafo del apartado 3 del artículo 20 queda redactado del siguiente modo:

«3. En el caso de que los estatutos establezcan la elección del Rector por la comunidad universitaria, el voto será ponderado por los distintos sectores de la comunidad universitaria. En todo caso, la mayoría corresponderá a los profesores doctores con vinculación permanente a la universidad.»

Veintiuno. El apartado 4 del artículo 20 queda sin contenido.

Veintidós. El artículo 22 queda redactado del siguiente modo:

«Artículo 22. *Secretario General.*

El Secretario, o la Secretaria General, que será nombrado por el Rector entre funcionarios públicos que presten servicios en la universidad, pertenecientes a cuerpos para cuyo ingreso se exija estar en posesión del título de Doctor, Licenciado, Ingeniero, Arquitecto o equivalente, lo será también del Consejo de Gobierno.»

Veintitrés. El artículo 23 queda redactado del siguiente modo:

«Artículo 23. *Gerente.*

Al o a la Gerente le corresponde la gestión de los servicios administrativos y económicos de la universidad. Será propuesto por el Rector y nombrado por éste de acuerdo con el Consejo Social, atendiendo a criterios de competencia profesional y experiencia. El Gerente no podrá ejercer funciones docentes.»

Veinticuatro. El artículo 24 queda redactado del siguiente modo:

«Artículo 24. *Decanos de Facultad y Directores de Escuela.*

Los Decanos y Decanas de Facultad y Directores y Directoras de Escuela ostentan la representación de sus centros y ejercen las funciones de dirección y gestión ordinaria de éstos. Serán elegidos, en los términos establecidos por los estatutos, entre los profesores y profesoras con vinculación permanente a la universidad.»

Veinticinco. El artículo 25 queda redactado del siguiente modo:

«Artículo 25. *Directores de Departamento.*

Los Directores y Directoras de Departamento ostentan la representación de éste y ejercen las funciones de dirección y gestión ordinaria del Departamento. Serán elegidos por el Consejo de Departamento en los términos establecidos por los estatutos, entre los profesores y profesoras doctores con vinculación permanente a la universidad.»

Veintiséis. El apartado 1 del artículo 27 queda redactado del siguiente modo:

«1. Las normas de organización y funcionamiento de las universidades privadas establecerán sus órganos de gobierno y representación, así como los procedimientos para su designación y remoción, asegurando en dichos órganos, mediante una participación adecuada, la representación de los diferentes sectores de la comunidad universitaria de forma que propicie la presencia equilibrada entre mujeres y hombres. En todo caso, las normas de organización y funcionamiento de las universidades privadas deberán garantizar que las decisiones de naturaleza estrictamente académica se adopten por órganos en los que el personal docente o investigador tenga una representación mayoritaria. Igualmente, deberán garantizar que el personal docente o investigador sea oído en el nombramiento del Rector.»

Veintisiete. El título IV queda redactado del siguiente modo:

«TÍTULO IV

De la coordinación universitaria

Artículo 27 bis. *Conferencia General de Política Universitaria.*

1. La Conferencia General de Política Universitaria, sin perjuicio de las funciones atribuidas a los órganos de coordinación universitaria de las Comunidades Autónomas, es el órgano de concertación, coordinación y cooperación de la política general universitaria al que le corresponden las funciones de:

a) Establecer y valorar las líneas generales de política universitaria, su articulación en el espacio europeo de educación superior y su interrelación con las políticas de investigación científica y tecnológica.

b) Planificación, informe, consulta y asesoramiento sobre la programación general y plurianual de la enseñanza universitaria, que comprende los recursos humanos, materiales y financieros precisos para la prestación del servicio público universitario.

c) Aprobar los criterios de coordinación sobre las actividades de evaluación, certificación y acreditación reguladas en el título V.

d) Proponer y valorar medidas para impulsar la colaboración entre universidad y empresa.

e) Coordinar la elaboración y seguimiento de informes sobre la aplicación del principio de igualdad de mujeres y hombres en la universidad.

En el desarrollo de sus funciones, podrá proponer que se soliciten informes o estudios del Consejo Económico y Social.

2. Bianualmente, la Conferencia General de Política Universitaria elaborará un informe sobre la situación del sistema universitario y su financiación, y formulará

propuestas que permitan mejorar su calidad y su eficiencia, asegurar la suficiencia financiera del mismo, así como garantizar a los ciudadanos las condiciones de igualdad en el ejercicio del derecho a la educación.

3. Bajo la presidencia del titular del departamento ministerial que tenga atribuidas las competencias en materia de universidades, estará compuesta por los responsables de la enseñanza universitaria en los Consejos de Gobierno de las Comunidades Autónomas y por cinco miembros designados por el presidente de la Conferencia.

4. La organización y el funcionamiento de la Conferencia se establecerán en su reglamento interno.

Artículo 28. *Consejo de Universidades.*

El Consejo de Universidades es el órgano de coordinación académica, así como de cooperación, consulta y propuesta en materia universitaria. Le corresponden las siguientes funciones, que desarrolla con plena autonomía funcional:

a) Servir de cauce para la colaboración, la cooperación y la coordinación en el ámbito académico.

b) Informar las disposiciones legales y reglamentarias que afectan al sistema universitario en su conjunto.

c) Prestar el asesoramiento que en materia universitaria sea requerido por el Ministerio de Educación y Ciencia, la Conferencia General de Política Universitaria o, en su caso, de las Comunidades Autónomas.

d) Formular propuestas al Gobierno, en materias relativas al sistema universitario y a la Conferencia General de Política Universitaria.

e) La verificación de la adecuación de los planes de estudios a las directrices y condiciones establecidas por el Gobierno para los títulos oficiales.

f) Desarrollar cuantas otras tareas le encomienden las leyes y sus disposiciones de desarrollo.

Artículo 29. *Composición del Consejo de Universidades.*

El Consejo de Universidades será presidido por el titular del Ministerio competente en materia de universidades y estará compuesto por los siguientes vocales:

a) Los Rectores de las universidades.

b) Cinco miembros designados por el Presidente del Consejo.

Artículo 30. *Organización del Consejo de Universidades.*

1. El Consejo de Universidades funcionará en pleno y en comisiones.

2. El Pleno, presidido por el Presidente del Consejo de Universidades o por el miembro en quien delegue, tendrá las siguientes funciones: elaborar el reglamento del Consejo y elevarlo al Ministro competente en materia de universidades para su aprobación por el Gobierno; proponer, en su caso, sus modificaciones; informar los criterios de coordinación sobre las actividades de evaluación, certificación y acreditación reguladas en el título V; elaborar la memoria anual del Consejo, y aquellas otras que se determinen en su reglamento.

3. Los distintos órganos del Consejo de Universidades podrán contar para el desarrollo de su trabajo con la colaboración de expertos y expertas en las materias que le son propias. La vinculación de estos expertos con el Consejo de Universidades podrá tener un carácter permanente o temporal, de acuerdo con lo que disponga su reglamento.

4. En los asuntos que afecten en exclusiva al sistema universitario público tendrán derecho a voto el Presidente del Consejo, los Rectores de las universidades públicas y los cinco miembros del Consejo designados por el Presidente.»

Veintiocho. El primer inciso y el párrafo a) del apartado 2 del artículo 31 quedan redactados del siguiente modo y se añaden un párrafo nuevo al final del apartado 3 y un apartado 4 con la siguiente redacción:

«2. Los objetivos señalados en el apartado anterior se cumplirán mediante el establecimiento de criterios comunes de garantía de calidad que faciliten la evaluación, la certificación y la acreditación de:

a) Las enseñanzas conducentes a la obtención de títulos de carácter oficial y validez en todo el territorio nacional.»

«3. ...

A tal fin, la Agencia Nacional de Evaluación de la Calidad y Acreditación y los órganos de evaluación creados por ley de las Comunidades Autónomas, de acuerdo con estándares internacionales de calidad, establecerán mecanismos de cooperación y reconocimiento mutuo. La Conferencia General de Política Universitaria informará y propondrá al Gobierno su regulación, a los efectos de garantizar el cumplimiento de los objetivos señalados en los apartados anteriores.

4. El Gobierno, previo informe de la Conferencia General de Política Universitaria, regulará las condiciones para que las universidades sometan a evaluación y seguimiento el desarrollo efectivo de las enseñanzas oficiales, así como el procedimiento para su acreditación.»

Veintinueve. El artículo 32 queda redactado del siguiente modo:

«Artículo 32. *Agencia Nacional de Evaluación de la Calidad y Acreditación.*

1. Se autoriza la creación de la Agencia Nacional de Evaluación de la Calidad y Acreditación, de acuerdo con las previsiones de la Ley de Agencias Estatales para la mejora de los servicios públicos, a la que corresponden las funciones que le atribuye la presente Ley y la de elevar informes al ministerio competente en materia de universidades y al Consejo de Universidades sobre el desarrollo de los procesos de evaluación, certificación y acreditación en España, a cuyos efectos podrá solicitar y prestar colaboración a los órganos de evaluación que, en su caso, existan en las Comunidades Autónomas.

2. La Agencia Nacional de Evaluación de la Calidad y Acreditación desarrollará su actividad de acuerdo con los principios de competencia técnica y científica, legalidad y seguridad jurídica, independencia y transparencia, atendiendo a los criterios de actuación usuales de estas instituciones en el ámbito internacional.»

Treinta. El artículo 34 queda redactado del siguiente modo:

«Artículo 34. *Títulos universitarios.*

1. Las universidades impartirán enseñanzas conducentes a la obtención de títulos oficiales y con validez en todo el territorio nacional y podrán impartir enseñanzas conducentes a la obtención de otros títulos.

2. Los títulos universitarios de carácter oficial y con validez en todo el territorio nacional deberán inscribirse en el Registro de universidades, centros y títulos, previsto en la disposición adicional vigésima. Podrán inscribirse otros títulos a efectos informativos. El Gobierno regulará el procedimiento y las condiciones para su inscripción.»

Treinta y uno. Se da nueva redacción al artículo 35:

«Artículo 35. *Títulos oficiales.*

1. El Gobierno establecerá las directrices y las condiciones para la obtención de los títulos universitarios de carácter oficial y con validez en todo el territorio nacional, que serán expedidos en nombre del Rey por el Rector de la universidad.

2. Para impartir enseñanzas oficiales y expedir los correspondientes títulos oficiales, con validez en todo el territorio nacional, las universidades deberán poseer

la autorización pertinente de la Comunidad Autónoma, según lo dispuesto en la legislación de la misma y lo previsto en el artículo 8 de esta Ley, y obtener la verificación del Consejo de Universidades de que el oportuno plan de estudios se ajusta a las directrices y condiciones establecidas por el Gobierno. El procedimiento deberá preservar la autonomía académica de las universidades.

3. Tras la autorización de la Comunidad Autónoma y la verificación del plan de estudios que otorgue el Consejo de Universidades, el Gobierno establecerá el carácter oficial del título y ordenará su inscripción en el Registro de universidades, centros y títulos.

4. Una vez que el Gobierno haya aprobado el carácter oficial de dicho título, el Rector ordenará publicar el plan de estudios en el ''Boletín Oficial del Estado'' y en el diario oficial de la Comunidad Autónoma.»

Treinta y dos. El artículo 36 queda redactado del siguiente modo:

«Artículo 36. *Convalidación o adaptación de estudios, validación de experiencia, equivalencia de títulos y homologación de títulos extranjeros.*

El Gobierno, previo informe del Consejo de Universidades, regulará:

a) Los criterios generales a que habrán de ajustarse las universidades en materia de convalidación y adaptación de estudios cursados en centros académicos españoles o extranjeros.

b) Las condiciones para la declaración de equivalencia de títulos españoles de enseñanza superior universitaria o no universitaria a aquéllos a que se refiere el artículo 35.

c) Las condiciones de homologación de títulos extranjeros de educación superior.

d) Las condiciones para validar, a efectos académicos, la experiencia laboral o profesional.

e) El régimen de convalidaciones entre los estudios universitarios y las otras enseñanzas de educación superior a las que se refiere el artículo 3.5 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación.»

Treinta y tres. Los artículos 37 y 38 quedan redactados del siguiente modo:

«Artículo 37. *Estructura de las enseñanzas oficiales.*

Las enseñanzas universitarias se estructurarán en tres ciclos: Grado, Máster y Doctorado. La superación de tales enseñanzas dará derecho, en los términos que establezca el Gobierno, previo informe del Consejo de Universidades, a la obtención de los títulos oficiales correspondientes.»

«Artículo 38. *Doctorado.*

Los estudios de doctorado, conducentes a la obtención del correspondiente título de carácter oficial y validez en todo el territorio nacional, que tienen como finalidad la especialización del estudiante en su formación investigadora dentro de un ámbito del conocimiento científico, técnico, humanístico o artístico, se organizarán y realizarán en la forma que determinen los estatutos, de acuerdo con los criterios que para la obtención del título de Doctor apruebe el Gobierno, previo informe del Consejo de Universidades. En todo caso, estos criterios incluirán la superación de un período de formación y la elaboración, presentación y aprobación de un trabajo original de investigación.»

Treinta y cuatro. El título VII pasa a denominarse «De la investigación en la universidad y de la transferencia del conocimiento».

Treinta y cinco. El artículo 39 pasa a titularse «La investigación y la transferencia del conocimiento. Funciones de la universidad».

Treinta y seis. El apartado 1 del artículo 39 queda redactado del siguiente modo:

«1. La investigación científica es fundamento esencial de la docencia y una herramienta primordial para el desarrollo social a través de la transferencia de sus

resultados a la sociedad. Como tal, constituye una función esencial de la universidad, que deriva de su papel clave en la generación de conocimiento y de su capacidad de estimular y generar pensamiento crítico, clave de todo proceso científico.»

Treinta y siete. El apartado 3 del artículo 39 queda redactado del siguiente modo:

«3. La universidad tiene, como uno de sus objetivos esenciales, el desarrollo de la investigación científica, técnica y artística y la transferencia del conocimiento a la sociedad, así como la formación de investigadores e investigadoras, y atenderá tanto a la investigación básica como a la aplicada.»

Treinta y ocho. Se añade un nuevo apartado 1 bis) al artículo 40 con la siguiente redacción y el apartado 3 del artículo 40 queda redactado del siguiente modo:

«1 bis) La universidad apoyará y promoverá la dedicación a la investigación de la totalidad del Personal Docente e Investigador permanente.»

«3. La actividad y dedicación investigadora y la contribución al desarrollo científico, tecnológico o artístico del personal docente e investigador de las universidades será criterio relevante, atendiendo su oportuna evaluación, para determinar su eficiencia en el desarrollo de su actividad profesional. La universidad facilitará la compatibilidad en el ejercicio de la docencia y la investigación e incentivará el desarrollo de una trayectoria profesional que permita una dedicación más intensa a la actividad docente o a la investigadora.»

Treinta y nueve. El apartado 1 del artículo 41 queda redactado del siguiente modo:

«1. La universidad desarrollará una investigación de calidad y una gestión eficaz de la transferencia del conocimiento y la tecnología, con los objetivos de contribuir al avance del conocimiento y del desarrollo tecnológico, la innovación y la competitividad de las empresas, la mejora de la calidad de vida de la ciudadanía, el progreso económico y social y un desarrollo responsable equitativo y sostenible, así como garantizar el fomento y la consecución de la igualdad.»

Cuarenta. La letra e) del apartado 2, del artículo 41 queda redactada del siguiente modo:

«e) La incorporación a las universidades de personal técnico de apoyo a la investigación, atendiendo a las características de los distintos campos científicos, así como del personal de administración y servicios especializado en la gestión de la investigación y el conocimiento.»

Cuarenta y uno. La letra g) del apartado 2, del artículo 41 queda redactada del siguiente modo:

«g) La vinculación entre la investigación universitaria y el sistema productivo, como vía para articular la transferencia de los conocimientos generados y la presencia de la universidad en el proceso de innovación del sistema productivo y de las empresas, prestando especial atención a la vinculación con el sistema productivo de su entorno. Dicha vinculación podrá, en su caso, llevarse a cabo a través de la creación de empresas de base tecnológica a partir de la actividad universitaria, en cuyas actividades podrá participar el personal docente e investigador de las universidades conforme al régimen previsto en el artículo 83.»

Cuarenta y dos. Se añaden los apartados 3 y 4 al artículo 41, con la siguiente redacción:

«3. La transferencia del conocimiento es una función de las universidades. Estas determinarán y establecerán los medios e instrumentos necesarios para facilitar la prestación de este servicio social por parte del personal docente e investigador.

El ejercicio de dicha actividad dará derecho a la evaluación de sus resultados y al reconocimiento de los méritos alcanzados, como criterio relevante para determinar su eficiencia en el desarrollo de su actividad profesional.

Las universidades fomentarán la cooperación con el sector productivo, de acuerdo con lo establecido en el artículo 83. A tal efecto, promoverán la movilidad del personal docente e investigador, así como el desarrollo conjunto de programas y proyectos de investigación y desarrollo tecnológico, la creación de centros o

estructuras mixtas y la pertenencia y participación activa en redes de conocimiento y plataformas tecnológicas.

4. Se promoverá que los equipos de investigación desarrollen su carrera profesional fomentando una presencia equilibrada entre mujeres y hombres en todos sus ámbitos.»

Cuarenta y tres. Se da nueva redacción al apartado 3 del artículo 42 y se añade un apartado 4 con la siguiente redacción:

«3. Corresponde al Gobierno, previo informe de la Conferencia General de Política Universitaria, establecer las normas básicas para la admisión de los estudiantes que soliciten ingresar en los centros universitarios, siempre con respeto a los principios de igualdad, mérito y capacidad. En todo caso, y de acuerdo con lo que establece el artículo 38 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, para acceder a los estudios universitarios será necesaria la superación de una única prueba.

La Conferencia General de Política Universitaria velará porque el procedimiento de admisión a los estudios universitarios de carácter oficial sea general, objetivo y universal, tenga validez en todas las universidades españolas y responda a criterios acordes con el espacio europeo de educación superior.

4. Para facilitar la actualización de la formación y la readaptación profesionales y la plena y efectiva participación en la vida cultural, económica y social, el Gobierno, previo informe del Consejo de Universidades, regulará los procedimientos para el acceso a la universidad de quienes, acreditando una determinada experiencia laboral o profesional, no dispongan de la titulación académica legalmente requerida al efecto con carácter general. A este sistema de acceso, que permitirá el ingreso en cualquier universidad, centro y enseñanza, podrán acogerse también, en las condiciones que al efecto se establezcan, quienes, no pudiendo acreditar dicha experiencia, hayan superado una determinada edad.»

Cuarenta y cuatro. El artículo 44 queda redactado del siguiente modo:

«Artículo 44. *Límites máximos de admisión de estudiantes.*

El Gobierno, previo acuerdo de la Conferencia General de Política Universitaria podrá, para poder cumplir las exigencias derivadas de Directivas comunitarias o de convenios internacionales, o bien por motivos de interés general igualmente acordados en la Conferencia General de Política Universitaria, establecer límites máximos de admisión de estudiantes en los estudios de que se trate. Dichos límites afectarán al conjunto de las universidades públicas y privadas.»

Cuarenta y cinco. El segundo párrafo del apartado 1 y los apartados 2 y 4 del artículo 45 quedan redactados del siguiente modo:

«1. ...

A estos efectos, el Gobierno determinará con carácter básico las modalidades y cuantías de las becas y ayudas al estudio, las condiciones académicas y económicas que hayan de reunir los candidatos, así como los supuestos de incompatibilidad, revocación y reintegro y cuantos requisitos, condiciones socioeconómicas u otros factores sean precisos para asegurar la igualdad en el acceso a las citadas becas y ayudas en todo el territorio, sin detrimento de las competencias normativas y de ejecución de las Comunidades Autónomas...»

«2. El desarrollo, ejecución y control del sistema general de becas y ayudas al estudio corresponde a las Comunidades Autónomas en sus respectivos ámbitos de competencia y en colaboración con las universidades, con el fin de facilitar la gestión descentralizada y la atención a las peculiaridades territoriales que la legislación contemple.

En todo caso, para asegurar que los resultados de la aplicación del sistema general de becas y ayudas al estudio propicien el derecho de todos los ciudadanos a la educación y garanticen el principio de igualdad en su obtención, se establecerán

los oportunos mecanismos de coordinación entre el Gobierno y las Comunidades Autónomas en el seno de la Conferencia General de Política Universitaria.»

«4. Con objeto de que nadie quede excluido del estudio en la universidad por razones económicas, el Gobierno y las Comunidades Autónomas, así como las propias universidades, instrumentarán una política de becas, ayudas y créditos para el alumnado y, en el caso de las universidades públicas, establecerán, asimismo, modalidades de exención parcial o total del pago de los precios públicos por prestación de servicios académicos. En todos los casos, se prestará especial atención a las personas con cargas familiares, víctimas de la violencia de género y personas con dependencia y discapacidad, garantizando así su acceso y permanencia a los estudios universitarios.»

Cuarenta y seis. El párrafo b) del apartado 2 del artículo 46 queda redactado del siguiente modo, y se añaden los párrafos i), j) y k), con la siguiente redacción:

«b) La igualdad de oportunidades y no discriminación por razones de sexo, raza, religión o discapacidad o cualquier otra condición o circunstancia personal o social en el acceso a la universidad, ingreso en los centros, permanencia en la universidad y ejercicio de sus derechos académicos.»

«i) Obtener reconocimiento académico por su participación en actividades universitarias culturales, deportivas, de representación estudiantil, solidarias y de cooperación.

j) Recibir un trato no sexista.

k) Una atención que facilite compaginar los estudios con la actividad laboral.»

Cuarenta y siete. Se añade un apartado 5 al artículo 46, con la siguiente redacción:

«5. El Gobierno aprobará un estatuto del estudiante universitario, que deberá prever la constitución, las funciones, la organización y el funcionamiento de un Consejo del estudiante universitario como órgano colegiado de representación estudiantil, adscrito al ministerio al que se le atribuyen las competencias en materia de universidades. La regulación del Consejo del estudiante universitario contará con la representación estudiantil de todas las universidades y, en su caso, con una adecuada participación de representantes de los consejos autonómicos de estudiantes.»

Cuarenta y ocho. El artículo 48 queda redactado del siguiente modo:

«Artículo 48. *Normas generales.*

1. Las universidades podrán contratar personal docente e investigador en régimen laboral, a través de las modalidades de contratación laboral específicas del ámbito universitario que se regulan en esta Ley o mediante las modalidades previstas en el Estatuto de los Trabajadores para la sustitución de trabajadores con derecho a reserva del puesto de trabajo. También podrán contratar personal investigador, técnico u otro personal, a través del contrato de trabajo por obra o servicio determinado, para el desarrollo de proyectos de investigación científica o técnica.

Asimismo, las universidades podrán nombrar profesoras y profesores eméritos en las condiciones previstas en esta Ley.

2. Las modalidades de contratación laboral específicas del ámbito universitario son las que se corresponden con las figuras de Ayudante, Profesor Ayudante Doctor, Profesor Contratado Doctor, Profesor Asociado y Profesor Visitante.

El régimen de las indicadas modalidades de contratación laboral será el que se establece en esta Ley y en sus normas de desarrollo; supletoriamente, será de aplicación lo dispuesto en el texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 1/1995, de 24 de marzo, y en sus normas de desarrollo.

3. La contratación de personal docente e investigador, excepto la figura de Profesor Visitante, se hará mediante concurso público, al que se dará la necesaria

publicidad y cuya convocatoria será comunicada con la suficiente antelación al Consejo de Universidades para su difusión en todas ellas. La selección se efectuará con respeto a los principios constitucionales de igualdad, mérito y capacidad. Se considerará mérito preferente estar acreditado o acreditada para participar en los concursos de acceso a los cuerpos docentes universitarios.

4. El personal docente e investigador contratado, computado en equivalencias a tiempo completo, no podrá superar el 49 por ciento del total de personal docente e investigador de la universidad. No se computará como profesorado contratado a quienes no impartan docencia en las enseñanzas conducentes a la obtención de los títulos oficiales así como al personal propio de los institutos de investigación adscritos a la universidad.

5. El personal docente e investigador con contrato laboral temporal no podrá superar el 40 por ciento de la plantilla docente.

6. En los términos de la presente Ley y en el marco de sus competencias, las Comunidades Autónomas establecerán el régimen del personal docente e investigador contratado de las universidades.»

Cuarenta y nueve. El artículo 49 queda redactado del siguiente modo:

«Artículo 49. *Ayudantes.*

La contratación de Ayudantes se ajustará a las siguientes reglas:

a) Las universidades podrán contratar como Ayudantes a quienes hayan sido admitidos o a quienes estén en condiciones de ser admitidos en los estudios de doctorado.

b) La finalidad principal del contrato será la de completar la formación docente e investigadora de dichas personas. Los Ayudantes colaborarán en tareas docentes de índole práctica hasta un máximo de 60 horas anuales.

c) El contrato será de carácter temporal y con dedicación a tiempo completo.

d) La duración del contrato no podrá ser inferior a un año ni superior a cinco, pudiendo prorrogarse o renovarse si se hubiera concertado por una duración inferior a la máxima, siempre que la duración total no exceda de los indicados cinco años. Las situaciones de incapacidad temporal, maternidad y adopción o acogimiento durante el período de duración del contrato, interrumpirán su cómputo.»

Cincuenta. El artículo 50 queda redactado del siguiente modo:

«Artículo 50. *Profesores Ayudantes Doctores.*

La contratación de Profesoras y Profesores Ayudantes Doctores se ajustará a las siguientes reglas:

a) El contrato se celebrará con doctores. La contratación exigirá la previa evaluación positiva de su actividad por parte de la Agencia Nacional de Evaluación de la Calidad y Acreditación o del órgano de evaluación externa que la ley de la Comunidad Autónoma determine, y será mérito preferente la estancia del candidato en universidades o centros de investigación de reconocido prestigio, españoles o extranjeros, distintos de la universidad que lleve a cabo la contratación.

b) La finalidad del contrato será la de desarrollar tareas docentes y de investigación.

c) El contrato será de carácter temporal y con dedicación a tiempo completo.

d) La duración del contrato no podrá ser inferior a un año ni superior a cinco, pudiendo prorrogarse o renovarse si se hubiera concertado por duración inferior a la máxima, siempre que la duración total no exceda de los indicados cinco años. En cualquier caso, el tiempo total de duración conjunta entre esta figura contractual y la prevista en el artículo anterior, en la misma o distinta universidad, no podrá exceder de ocho años. Las situaciones de incapacidad temporal, maternidad y adopción o acogimiento durante el período de duración del contrato, interrumpirán su cómputo.»

Cincuenta y uno. El artículo 51 queda sin contenido.

Cincuenta y dos. El artículo 52 queda redactado del siguiente modo:

«Artículo 52. *Profesores Contratados Doctores.*

La contratación de Profesoras y Profesores Contratados Doctores se ajustará a las siguientes reglas:

a) El contrato se celebrará con doctores que reciban la evaluación positiva por parte de la Agencia Nacional de Evaluación de la Calidad y Acreditación o del órgano de evaluación externo que la ley de la Comunidad Autónoma determine.

b) La finalidad del contrato será la de desarrollar, con plena capacidad docente e investigadora, tareas de docencia y de investigación, o prioritariamente de investigación.

c) El contrato será de carácter indefinido y con dedicación a tiempo completo.»

Cincuenta y tres. El artículo 53 queda redactado del siguiente modo:

«Artículo 53. *Profesores Asociados.*

La contratación de Profesoras y Profesores Asociados se ajustará a las siguientes reglas:

a) El contrato se podrá celebrar con especialistas de reconocida competencia que acrediten ejercer su actividad profesional fuera del ámbito académico universitario.

b) La finalidad del contrato será la de desarrollar tareas docentes a través de las que aporten sus conocimientos y experiencia profesionales a la universidad.

c) El contrato será de carácter temporal y con dedicación a tiempo parcial.

d) La duración del contrato será trimestral, semestral o anual, y se podrá renovar por períodos de igual duración, siempre que se siga acreditando el ejercicio de la actividad profesional fuera del ámbito académico universitario.»

Cincuenta y cuatro. El artículo 54 queda redactado del siguiente modo:

«Artículo 54. *Profesores Visitantes.*

La contratación de Profesoras y Profesores Visitantes se ajustará a las siguientes reglas:

a) El contrato se podrá celebrar con profesores o investigadores de reconocido prestigio de otras universidades y centros de investigación, tanto españoles como extranjeros.

b) La finalidad del contrato será la de desarrollar tareas docentes o investigadoras a través de las que se aporten los conocimientos y la experiencia docente e investigadora de los indicados profesores a la universidad.

c) El contrato será de carácter temporal con la duración que se acuerde entre las partes y dedicación a tiempo parcial o completo.»

Cincuenta y cinco. Se añade un artículo 54 bis con la siguiente redacción:

«Artículo 54 bis. *Profesores Eméritos.*

Las universidades, de acuerdo con sus estatutos, podrán nombrar a Profesores Eméritos entre profesoras y profesores jubilados que hayan prestado servicios destacados a la universidad.»

Cincuenta y seis. El apartado 2 del artículo 55 queda redactado del siguiente modo:

«2. Las Comunidades Autónomas podrán, asimismo, establecer retribuciones adicionales ligadas a méritos individuales por el ejercicio de las siguientes funciones: actividad y dedicación docente, formación docente, investigación, desarrollo tecnológico, transferencia de conocimientos y gestión. Dentro de los límites que para este fin fijen las Comunidades Autónomas, el Consejo Social, a propuesta del

Consejo de Gobierno, podrá acordar la asignación singular e individual de dichos complementos retributivos.»

Cincuenta y siete. El apartado 3 del artículo 55 queda redactado del siguiente modo:

«3. Sin perjuicio de lo dispuesto en el apartado anterior, el Gobierno podrá establecer programas de incentivos para la docencia, la investigación, el desarrollo tecnológico y la transferencia de conocimiento por el ejercicio de las funciones a que se refiere el apartado anterior, que comprendan al personal docente e investigador contratado.»

Cincuenta y ocho. El apartado 4 del artículo 55 queda redactado del siguiente modo:

«4. Los complementos retributivos derivados del desarrollo de los dos apartados anteriores se asignarán previa valoración de los méritos por parte del órgano de evaluación externo que la ley de la Comunidad Autónoma determine en el caso de los del apartado 2 y de la Agencia Nacional de Evaluación de la Calidad y Acreditación en el caso del apartado 3.»

Cincuenta y nueve. Los apartados 1 y 2 del artículo 56 quedan redactados del siguiente modo:

«1. El profesorado universitario funcionario pertenecerá a los siguientes cuerpos docentes:

a) Catedráticos de Universidad.
b) Profesores Titulares de Universidad.

El profesorado perteneciente a ambos cuerpos tendrá plena capacidad docente e investigadora.»

«2. El profesorado funcionario se regirá por las bases establecidas en esta Ley y en su desarrollo, por las disposiciones que, en virtud de sus competencias, dicten las Comunidades Autónomas, por la legislación general de funcionarios que les sea de aplicación y por los estatutos.»

Sesenta. El artículo 57 queda redactado del siguiente modo:

«Artículo 57. *Acreditación nacional.*

1. El acceso a los cuerpos de funcionarios docentes universitarios mencionados en el artículo 56.1 exigirá la previa obtención de una acreditación nacional que, valorando los méritos y competencias de los aspirantes, garantice la calidad en la selección del profesorado funcionario.

El Gobierno, previo informe del Consejo de Universidades, regulará el procedimiento de acreditación que, en todo caso, estará regido por los principios de publicidad, mérito y capacidad, en orden a garantizar una selección eficaz, eficiente, transparente y objetiva del profesorado funcionario, de acuerdo con los estándares internacionales evaluadores de la calidad docente e investigadora.

2. La acreditación será llevada a cabo mediante el examen y juicio sobre la documentación presentada por los solicitantes, por comisiones compuestas por al menos siete profesoras y profesores de reconocido prestigio docente e investigador contrastado pertenecientes a los cuerpos de funcionarios docentes universitarios. Tales profesores deberán ser Catedráticos para la acreditación al cuerpo de Catedráticos de Universidad, y Catedráticos y Profesores Titulares para la acreditación al cuerpo de Profesores Titulares de Universidad. Igualmente, podrán formar parte de estas comisiones expertos de reconocido prestigio internacional o pertenecientes a centros públicos de investigación.

Los currículos de los miembros de las comisiones de acreditación se harán públicos tras su nombramiento.

Reglamentariamente, se establecerá la composición de las comisiones reguladas en este apartado, la forma de determinación de sus componentes, así como su procedimiento de actuación y los plazos para resolver. En todo caso, deberá ajustarse a los principios de imparcialidad y profesionalidad de sus miembros,

procurando una composición equilibrada entre mujeres y hombres, salvo que no sea posible por razones fundadas y objetivas, debidamente motivadas.

3. En los supuestos de evaluación negativa, y con carácter previo a la resolución de la comisión, los interesados podrán presentar las alegaciones que consideren oportunas.

4. Una vez finalizado el procedimiento, se expedirá a favor del aspirante el correspondiente documento de acreditación.»

Sesenta y uno. El artículo 58 queda sin contenido.

Sesenta y dos. El artículo 59 queda redactado del siguiente modo:

«Artículo 59. *Acreditación para Profesores Titulares de universidad.*

1. Quienes posean el título de Doctor podrán presentar una solicitud para obtener la acreditación para Profesora o Profesor Titular de universidad a la que acompañarán, de acuerdo con lo que se establezca reglamentariamente, una justificación de los méritos que aduzcan.

2. Las comisiones nombradas conforme indica el artículo 57.2 examinarán los méritos presentados por los solicitantes y podrán recabar de ellos aclaraciones o justificaciones adicionales que se entregarán por escrito en el plazo que se establezca.»

Sesenta y tres. El artículo 60 queda redactado del siguiente modo:

«Artículo 60. *Acreditación para Catedráticos de universidad.*

1. Los funcionarios del Cuerpo de Profesores Titulares de Universidad podrán presentar una solicitud para obtener la acreditación para Catedrático o Catedrática de universidad a la que acompañarán, de acuerdo con lo que se establezca reglamentariamente, una justificación de los méritos que aduzcan.

Quedarán eximidos del requisito de pertenecer al Cuerpo de Profesores Titulares de Universidad quienes acrediten tener la condición de Doctor con, al menos, ocho años de antigüedad y obtengan el informe positivo de su actividad docente e investigadora, de acuerdo con el procedimiento que establezca el Gobierno.

2. Las comisiones nombradas conforme indica el artículo 57.2 examinarán los méritos presentados por los solicitantes y podrán recabar de ellos aclaraciones o justificaciones adicionales que se entregarán por escrito en el plazo que se establezca.»

Sesenta y cuatro. El artículo 62 queda redactado del siguiente modo:

«Artículo 62. *Concursos para el acceso a plazas de los cuerpos docentes universitarios.*

1. Las universidades, de acuerdo con lo que establezcan sus estatutos, convocarán concursos para el acceso a plazas de los cuerpos docentes universitarios que estén dotadas en el estado de gastos de su presupuesto. La convocatoria deberá ser publicada en el ''Boletín Oficial del Estado'' y en el de la Comunidad Autónoma. Los plazos para la presentación a los concursos contarán desde el día siguiente al de su publicación en el ''Boletín Oficial del Estado''.

2. A los concursos podrán presentarse quienes hayan sido acreditados de acuerdo con lo regulado, para cada caso, en los artículos 59 y 60, así como los funcionarios y funcionarias de los Cuerpos de Profesores Titulares de Universidad y de Catedráticos de Universidad.

3. Los estatutos de cada universidad regularán la composición de las comisiones de selección de las plazas convocadas y garantizarán, en todo caso, la necesaria aptitud científica y docente de sus componentes. Dicha composición deberá ajustarse a los principios de imparcialidad y profesionalidad de sus miembros, procurando una composición equilibrada entre mujeres y hombres, salvo que no sea posible por razones fundadas y objetivas debidamente motivadas. En cualquier caso,

los miembros de las comisiones deberán reunir los requisitos indicados en el artículo 57.2 y sus currículos deberán hacerse públicos.

4. Igualmente, los estatutos regularán el procedimiento que ha de regir en los concursos, que deberá valorar, en todo caso, el historial académico, docente e investigador del candidato o candidata, su proyecto docente e investigador, así como contrastar sus capacidades para la exposición y debate en la correspondiente materia o especialidad en sesión pública.

5. El proceso podrá concluir con la decisión de la comisión de no proveer la plaza convocada.»

Sesenta y cinco. El artículo 63 queda sin contenido.

Sesenta y seis. El artículo 64 queda redactado del siguiente modo:

«Artículo 64. *Garantías de las pruebas.*

1. En los concursos de acceso quedarán garantizados, en todo momento, la igualdad de oportunidades de los candidatos y el respeto a los principios de mérito y capacidad.

2. En los concursos de acceso, las universidades harán pública la composición de las comisiones, así como los criterios para la adjudicación de las plazas. Una vez celebrados, harán públicos los resultados de la evaluación de cada candidato, desglosada por cada uno de los aspectos evaluados.»

Sesenta y siete. El artículo 65 queda redactado del siguiente modo:

«Artículo 65. *Nombramientos.*

1. Las comisiones que juzguen los concursos de acceso propondrán al Rector, motivadamente y con carácter vinculante, una relación de todos los candidatos y candidatas por orden de preferencia para su nombramiento y sin que se pueda exceder en la propuesta el número de plazas convocadas a concurso. El Rector procederá a los nombramientos conforme a la propuesta realizada, ordenará su inscripción en el correspondiente registro de personal y su publicación en el ‘’Boletín Oficial del Estado’’ y en el de la Comunidad Autónoma, así como su comunicación al Consejo de Universidades.

2. La plaza obtenida tras el concurso de acceso deberá desempeñarse durante dos años, al menos, antes de poder participar en un nuevo concurso para obtener una plaza en otra universidad.»

Sesenta y ocho. El artículo 66 queda redactado del siguiente modo:

«Artículo 66. *Comisiones de reclamaciones.*

1. Contra las propuestas de las comisiones de acreditación, los solicitantes podrán presentar una reclamación ante el Consejo de Universidades. Admitida la reclamación, será valorada por una comisión, cuya composición se determinará reglamentariamente. Esta comisión examinará el expediente relativo a la acreditación para velar por las garantías establecidas y podrá ratificar la propuesta o, en su caso, admitir la reclamación, todo ello en un plazo máximo de tres meses. El transcurso del plazo establecido sin resolver se entenderá como rechazo de la reclamación presentada.

2. Contra las propuestas de las comisiones de los concursos de acceso, los concursantes podrán presentar una reclamación ante el Rector. Admitida a trámite la reclamación, se suspenderán los nombramientos hasta su resolución.

La reclamación será valorada por una comisión compuesta por siete Catedráticos de universidad pertenecientes a diversos ámbitos del conocimiento, designados en la forma que establezcan los estatutos, con amplia experiencia docente e investigadora.

Esta comisión examinará el expediente relativo al concurso para velar por las garantías establecidas y ratificará o no la propuesta reclamada en el plazo máximo de tres meses, tras lo que el Rector dictará la resolución en congruencia con lo que

indique la comisión. El transcurso del plazo establecido sin resolver se entenderá como rechazo de la reclamación presentada.

3. Las resoluciones del Consejo de Universidades y del Rector a que se refieren los apartados anteriores agotan la vía administrativa y serán impugnables directamente ante la jurisdicción contencioso-administrativa, de acuerdo con lo establecido en la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.»

Sesenta y nueve. El primer párrafo del artículo 67 queda redactado del siguiente modo:

«El reingreso al servicio activo de los funcionarios y funcionarias de cuerpos docentes universitarios en situación de excedencia voluntaria se efectuará mediante la obtención de una plaza en los concursos de acceso a los cuerpos docentes universitarios que cualquier universidad convoque, de acuerdo con lo establecido en el artículo 62.»

Setenta. El apartado 1 del artículo 68 queda redactado del siguiente modo:

«1. El profesorado de las universidades públicas ejercerá sus funciones preferentemente en régimen de dedicación a tiempo completo, o bien a tiempo parcial. La dedicación será, en todo caso, compatible con la realización de trabajos científicos, técnicos o artísticos a que se refiere el artículo 83.»

Setenta y uno. El apartado 1 del artículo 69 queda redactado del siguiente modo:

«1. El Gobierno determinará el régimen retributivo del personal docente e investigador universitario perteneciente a los cuerpos de funcionarios. Dicho régimen será el establecido por la legislación general de funcionarios, adecuado, específicamente a las características de dicho personal. A estos efectos, el Gobierno establecerá los intervalos de niveles o categorías dentro de cada nivel correspondientes a cada cuerpo docente, los requisitos de promoción de uno a otro, así como sus consecuencias retributivas.»

Setenta y dos El apartado 2 del artículo 69 queda redactado del siguiente modo:

«2. El Gobierno podrá establecer retribuciones adicionales a las anteriores ligadas a méritos individuales por el ejercicio de las siguientes funciones: actividad y dedicación docente, formación docente, investigación, desarrollo tecnológico, transferencia de conocimiento y gestión.»

Setenta y tres. El apartado 3 del artículo 69 queda redactado del siguiente modo:

«3. Las Comunidades Autónomas podrán, asimismo, establecer retribuciones adicionales ligadas a méritos individuales docentes, investigadores, de desarrollo tecnológico, de transferencia de conocimiento y de gestión por el ejercicio de las funciones a las que se refieren los artículos 33, 41.2 y 3. Dentro de los límites que para este fin fijen las Comunidades Autónomas, el Consejo Social, a propuesta del Consejo de Gobierno de la universidad, podrá acordar la asignación singular e individual de dichos complementos retributivos.»

Setenta y cuatro. El apartado 2 del artículo 72 queda redactado del siguiente modo:

«2. Con independencia de las condiciones generales que se establezcan de conformidad con el artículo 4.3, al menos el 50 por ciento del total del profesorado deberá estar en posesión del título de Doctor y, al menos, el 60 por ciento del total de su profesorado doctor deberá haber obtenido la evaluación positiva de la Agencia Nacional de Evaluación de la Calidad y Acreditación o del órgano de evaluación externa que la ley de la Comunidad Autónoma determine. A estos efectos, el número total de Profesores se computará sobre el equivalente en dedicación a tiempo completo. Los mismos requisitos serán de aplicación a los centros universitarios privados adscritos a universidades privadas.»

Setenta y cinco. Se añade un apartado 3 al artículo 72, con la siguiente redacción:

«3. El profesorado de las universidades privadas y de los centros privados de enseñanza universitaria adscritos a universidades, no podrá ser funcionario de un cuerpo docente universitario en situación de activo y destino en una universidad pública. La misma limitación se aplicará al personal docente e investigador a tiempo completo.»

Setenta y seis. El apartado 2 del artículo 73 queda redactado del siguiente modo:

«2. Corresponde al personal de administración y servicios la gestión técnica, económica y administrativa, así como el apoyo, asesoramiento y asistencia en el desarrollo de las funciones de la universidad.

Corresponde al personal de administración y servicios de las universidades públicas el apoyo, asistencia y asesoramiento a las autoridades académicas, el ejercicio de la gestión y administración, particularmente en las áreas de recursos humanos, organización administrativa, asuntos económicos, informática, archivos, bibliotecas, información, servicios generales, servicios científico-técnicos, así como el soporte a la investigación y la transferencia de tecnología y a cualesquiera otros procesos de gestión administrativa y de soporte que se determine necesario para la universidad en el cumplimiento de sus objetivos.»

Setenta y siete. Se añade un punto 3 al artículo 74 con el siguiente texto:

«3. El Gobierno y las Comunidades Autónomas podrán establecer programas de incentivos ligados a méritos individuales vinculados a su contribución en la mejora de la investigación y la transferencia de conocimiento.»

Setenta y ocho. El artículo 76 queda redactado del siguiente modo, y se añade un nuevo artículo 76 bis con la siguiente redacción:

«Artículo 76. *Provisión de las plazas.*

1. La provisión de puestos de personal de administración y servicios de las universidades se realizará por el sistema de concursos, a los que podrán concurrir tanto el personal propio de aquéllas como el personal de otras universidades. El personal perteneciente a cuerpos y escalas de las Administraciones públicas podrá concurrir en las condiciones que reglamentariamente se determinen.

2. Sólo podrán cubrirse por el sistema de libre designación aquellos puestos que se determinen por las universidades atendiendo a la naturaleza de sus funciones, y de conformidad con la normativa general de la función pública.

3. Los estatutos establecerán las normas para asegurar la provisión de las vacantes que se produzcan y el perfeccionamiento y promoción profesional del personal, de acuerdo con los principios de publicidad, igualdad, mérito y capacidad.»

«Artículo 76 bis. *Formación y movilidad.*

1. Las universidades fomentarán la formación permanente del personal de administración y servicios. A tal efecto, facilitarán que dicho personal pueda seguir programas que aumenten sus habilidades y competencias profesionales.

2. Las universidades promoverán las condiciones para que el personal de administración y servicios pueda desempeñar sus funciones en universidades distintas de la de origen. A tal fin, podrán formalizarse convenios entre las universidades o con otras Administraciones públicas que garanticen el derecho a la movilidad de su respectivo personal bajo el principio de reciprocidad.»

Setenta y nueve. El apartado 1 del artículo 79 queda redactado del siguiente modo:

«1. Las universidades públicas tendrán autonomía económica y financiera en los términos establecidos en la presente Ley. A tal efecto, se garantizará que las universidades dispongan de los recursos necesarios para un funcionamiento básico de calidad.»

Ochenta. Se añade un apartado 3 al artículo 83, con la siguiente redacción:

«3. Siempre que una empresa de base tecnológica sea creada o desarrollada a partir de patentes o de resultados generados por proyectos de investigación financiados total o parcialmente con fondos públicos y realizados en universidades, el profesorado funcionario de los cuerpos docentes universitarios y el contratado con vinculación permanente a la universidad que fundamente su participación en los mencionados proyectos podrán solicitar la autorización para incorporarse a dicha empresa, mediante una excedencia temporal.

El Gobierno, previo informe de la Conferencia General de Política Universitaria, regulará las condiciones y el procedimiento para la concesión de dicha excedencia que, en todo caso, sólo podrá concederse por un límite máximo de cinco años. Durante este período, los excedentes tendrán derecho a la reserva del puesto de trabajo y a su cómputo a efectos de antigüedad. Si con anterioridad a la finalización del período por el que se hubiera concedido la excedencia el profesor no solicitara el reingreso al servicio activo, será declarado de oficio en situación de excedencia voluntaria por interés particular.»

Ochenta y uno. El título XIII queda redactado del siguiente modo:

«TÍTULO XIII

Espacio europeo de enseñanza superior

Artículo 87. *De la integración en el espacio europeo de enseñanza superior.*

En el ámbito de sus respectivas competencias el Gobierno, las Comunidades Autónomas y las universidades adoptarán las medidas necesarias para completar la plena integración del sistema español en el espacio europeo de enseñanza superior.

Artículo 88. *De las enseñanzas y títulos y de la movilidad de estudiantes.*

1. A fin de promover la más amplia movilidad de estudiantes y titulados españoles en el espacio europeo de enseñanza superior, el Gobierno, previo informe del Consejo de Universidades, adoptará las medidas que aseguren que los títulos oficiales expedidos por las universidades españolas se acompañen del suplemento europeo al título.

2. Asimismo, el Gobierno, previo informe del Consejo de Universidades, establecerá las normas necesarias para que la unidad de medida del haber académico, correspondiente a la superación de cada una de las materias que integran los planes de estudio de las diversas enseñanzas conducentes a la obtención de títulos de carácter oficial y validez en todo el territorio nacional, sea el crédito europeo.

3. El Gobierno, las Comunidades Autónomas y las universidades fomentarán la movilidad de los estudiantes en el espacio europeo de enseñanza superior a través de programas de becas y ayudas y créditos al estudio o, en su caso, complementando los programas de becas y ayudas de la Unión Europea.

Artículo 89. *Del Profesorado.*

1. El profesorado de las universidades de los Estados miembros de la Unión Europea que haya alcanzado en aquéllas una posición equivalente a las de Catedrático o Profesor Titular de universidad será considerado acreditado a los efectos previstos en esta Ley, según el procedimiento y condiciones que se establezcan reglamentariamente por el Gobierno, previo informe del Consejo de Universidades.

2. El profesorado al que se refiere el apartado 1 podrá formar parte de las comisiones a que se refiere el artículo 57 y, si las universidades así lo establecen en sus estatutos, de las comisiones encargadas de resolver los concursos para el acceso a los cuerpos docentes universitarios.

3. A los efectos de la concurrencia a los procedimientos de acreditación, a los concursos de acceso a los cuerpos de funcionarios docentes universitarios y a las convocatorias de contratos de profesorado que prevé esta Ley, los nacionales de los Estados miembros de la Unión Europea gozarán de idéntico tratamiento, y con los mismos efectos, al de los nacionales españoles.

Lo establecido en el párrafo anterior será de aplicación a los nacionales de aquellos Estados a los que, en virtud de tratados internacionales celebrados por la Unión Europea y ratificados por España, sea de aplicación la libre circulación de trabajadores en los términos en que ésta se encuentra definida en el Tratado constitutivo de la Comunidad Europea.

4. El Gobierno, las Comunidades Autónomas y las universidades fomentarán la movilidad de los profesores en el espacio europeo de enseñanza superior a través de programas y convenios específicos y de los programas de la Unión Europea.

5. El Gobierno, las Comunidades Autónomas y las universidades impulsarán la realización de programas dirigidos a la renovación metodológica de la enseñanza universitaria para el cumplimiento de los objetivos de calidad del Espacio Europeo de Educación Superior.

Artículo 89 bis. *Del personal de administración y servicios.*

El Gobierno, las Comunidades Autónomas y las universidades fomentarán la movilidad del personal de administración y servicios en el Espacio Europeo de Enseñanza Superior a través de programas y convenios específicos, y en su caso, de los que instituya la Unión Europea.»

Ochenta y dos. Se añade un título XIV con la siguiente redacción:

«TÍTULO XIV

Del deporte y la extensión universitaria

Artículo 90. *Del deporte en la universidad.*

1. La práctica deportiva en la universidad es parte de la formación del alumnado y se considera de interés general para todos los miembros de la comunidad universitaria. Corresponde a las universidades en virtud de su autonomía la ordenación y organización de actividades y competiciones deportivas en su ámbito respectivo.

2. Las universidades establecerán las medidas oportunas para favorecer la práctica deportiva de los miembros de la comunidad universitaria y, en su caso, proporcionarán instrumentos para la compatibilidad efectiva de esa práctica con la formación académica de los estudiantes.

Artículo 91. *Coordinación en materia de deporte universitario.*

1. Corresponde a las Comunidades Autónomas la coordinación en materia de deporte universitario en el ámbito de su territorio.

2. Sin perjuicio de las competencias de las Comunidades Autónomas, el Gobierno, previo informe del Consejo de Universidades y a propuesta de la Conferencia General de Política Universitaria, dictará las disposiciones necesarias para la coordinación general de las actividades deportivas de las universidades y articulará fórmulas para compatibilizar los estudios de deportistas de alto nivel con sus actividades deportivas.

Artículo 92. *De la cooperación internacional y la solidaridad.*

Las universidades fomentarán la participación de los miembros de la comunidad universitaria en actividades y proyectos de cooperación internacional y solidaridad. Asimismo, propiciarán la realización de actividades e iniciativas que contribuyan al

impulso de la cultura de la paz, el desarrollo sostenible y el respeto al medio ambiente, como elementos esenciales para el progreso solidario.

Artículo 93. *De la cultura universitaria.*

Es responsabilidad de la universidad conectar al universitario con el sistema de ideas vivas de su tiempo. A tal fin, las universidades arbitrarán los medios necesarios para potenciar su compromiso con la reflexión intelectual, la creación y la difusión de la cultura. Específicamente las universidades promoverán el acercamiento de las culturas humanística y científica y se esforzarán por transmitir el conocimiento a la sociedad mediante la divulgación de la ciencia.»

Ochenta y tres. Se añade un apartado 4 a la disposición adicional segunda, con la siguiente redacción:

«4. El recurso al endeudamiento por parte de la Universidad Nacional de Educación a Distancia habrá de autorizarse por una norma con rango de ley. No obstante, a lo largo del ejercicio presupuestario, para atender desfases temporales de tesorería, la Universidad Nacional de Educación a Distancia podrá recurrir a la contratación de pólizas de crédito o préstamos, en una cuantía que no superará el cinco por ciento de su presupuesto, que habrán de quedar cancelados antes del 31 de diciembre de cada año.»

Ochenta y cuatro. El apartado 2 de la disposición adicional quinta queda redactado del siguiente modo:

«2. El funcionamiento de los colegios mayores o residencias se regulará por los estatutos de cada universidad y los propios de cada colegio mayor o residencia y gozarán de los beneficios o exenciones fiscales de la universidad a la que estén adscritos.»

Ochenta y cinco. La disposición adicional octava queda redactada del siguiente modo:

«Disposición adicional octava. *Del modelo de financiación de las Universidades públicas.*

En el plazo máximo de un año, la Conferencia General de Política Universitaria, previo informe del Consejo de Universidades, elaborará un modelo referencial de costes que facilite a los poderes públicos el establecimiento de una financiación adecuada de las universidades públicas que, atendiendo a lo previsto en el artículo 79.1, favorezca su plena participación en el Espacio Europeo de Educación Superior.»

Ochenta y seis. La disposición adicional decimoquinta queda redactada del siguiente modo:

«Disposición adicional decimoquinta. *Del acceso a los distintos ciclos de los estudios universitarios.*

En las directrices y condiciones previstas en el artículo 35.1, el Gobierno, previo informe del Consejo de Universidades, establecerá las condiciones para el paso de un ciclo a otro de aquéllos en que se estructuran los estudios universitarios de acuerdo con lo establecido en el artículo 37, así como para el acceso a los distintos ciclos desde enseñanzas o titulaciones universitarias o no universitarias que hayan sido declaradas equivalentes a las universitarias a todos los efectos.»

Ochenta y siete. La disposición adicional decimoséptima queda sin contenido.

Ochenta y ocho. La disposición adicional decimonovena queda redactada del siguiente modo:

«Disposición adicional decimonovena. *De las denominaciones.*

1. Sólo podrá utilizarse la denominación de universidad, o las propias de los centros, enseñanzas, títulos de carácter oficial y validez en todo el territorio nacional y órganos unipersonales de gobierno a que se refiere esta Ley, cuando hayan sido autorizadas o reconocidas de acuerdo con lo dispuesto en la misma. No podrán utilizarse aquellas otras denominaciones que, por su significado, puedan inducir a confusión con aquéllas.

2. Se declara la utilidad pública de los nombres de dominio de Internet de segundo nivel bajo el dominio ''.es'' correspondientes a las denominaciones a las que se refiere el apartado 1.»

Ochenta y nueve. La disposición adicional vigésima queda redactada del siguiente modo:

«Disposición adicional vigésima. *Registro de universidades, centros y títulos.*

En el Ministerio de Educación y Ciencia existirá el Registro de universidades, centros y títulos. Este registro tendrá carácter público y en él se inscribirán, además de las universidades y centros, los títulos oficiales con validez en todo el territorio nacional. Podrán inscribirse también otros títulos a efectos informativos que expidan las universidades. El Gobierno regulará su régimen, organización y funcionamiento.»

Noventa. La disposición adicional vigésima cuarta queda redactada del siguiente modo:

«Disposición adicional vigésima cuarta. *De la inclusión de las personas con discapacidad en las universidades.*

1. Las Universidades garantizarán la igualdad de oportunidades de los estudiantes y demás miembros de la comunidad universitaria con discapacidad, proscribiendo cualquier forma de discriminación y estableciendo medidas de acción positiva tendentes a asegurar su participación plena y efectiva en el ámbito universitario.

2. Los estudiantes y los demás miembros con discapacidad de la comunidad universitaria no podrán ser discriminados por razón de su discapacidad ni directa ni indirectamente en el acceso, el ingreso, la permanencia y el ejercicio de los títulos académicos y de otra clase que tengan reconocidos.

3. Las universidades promoverán acciones para favorecer que todos los miembros de la comunidad universitaria que presenten necesidades especiales o particulares asociadas a la discapacidad dispongan de los medios, apoyos y recursos que aseguren la igualdad real y efectiva de oportunidades en relación con los demás componentes de la comunidad universitaria.

4. Los edificios, instalaciones y dependencias de las universidades, incluidos también los espacios virtuales, así como los servicios, procedimientos y el suministro de información, deberán ser accesibles para todas las personas, de forma que no se impida a ningún miembro de la comunidad universitaria, por razón de discapacidad, el ejercicio de su derecho a ingresar, desplazarse, permanecer, comunicarse, obtener información u otros de análoga significación en condiciones reales y efectivas de igualdad.

Los entornos universitarios deberán ser accesibles de acuerdo con las condiciones y en los plazos establecidos en la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y en sus disposiciones de desarrollo.

5. Todos los planes de estudios propuestos por las universidades deben tener en cuenta que la formación en cualquier actividad profesional debe realizarse desde el respeto y la promoción de los Derechos Humanos y los principios de accesibilidad universal y diseño para todos.

6. Con arreglo a lo establecido en el artículo 30 de la Ley 13/1982, de 7 de abril, de Integración Social de los Minusválidos y en sus normas de desarrollo, los estudiantes con discapacidad, considerándose por tales aquellos comprendidos en el artículo 1.2 de la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no

discriminación y accesibilidad universal de las personas con discapacidad tendrán derecho a la exención total de tasas y precios públicos en los estudios conducentes a la obtención de un título universitario.»

Noventa y uno. El apartado 2 de la disposición adicional vigésima quinta queda redactado del siguiente modo:

«2. Para el acceso directo a la universidad de los titulados de Formación Profesional se estará a lo previsto en la Ley Orgánica 2/2006, de 3 de mayo, de Educación.»

Noventa y dos. La disposición adicional vigésima sexta queda sin contenido.

Noventa y tres. Se añade una disposición adicional vigésima octava con la siguiente redacción:

«Disposición adicional vigésima octava. *Disponibilidades económicas.*

El desarrollo temporal de la implantación de las medidas previstas en los artículos 55.3 y 69.2 se hará en función de las disponibilidades económicas de las instituciones responsables de la enseñanza universitaria.»

Noventa y cuatro. Se añade una nueva disposición adicional vigésima novena con la siguiente redacción:

«Disposición adicional vigésima novena. *Funciones de tutoría.*

Sin perjuicio de lo establecido en el artículo 72.3 los profesores de universidades públicas podrán realizar funciones de tutoría en universidades no presenciales públicas o financiadas mayoritariamente por Administraciones públicas, en la forma que se determine reglamentariamente.»

Noventa y cinco. Se da una nueva redacción a las disposiciones transitorias cuarta y quinta:

«Disposición transitoria cuarta. *Profesores con contrato administrativo LRU.*

Quienes a la entrada en vigor de la presente Ley se hallen contratados en universidades públicas como profesores con contrato administrativo LRU, podrán permanecer en su misma situación hasta la extinción del contrato y de su eventual renovación, conforme a la legislación que les venía siendo aplicable. No obstante, dichos contratos podrán ser prorrogados sin que su permanencia en esta situación pueda prorrogarse más de cinco años después de la entrada en vigor de la Ley.

Hasta ese momento, las universidades, previa solicitud de los interesados, podrán adaptar sus contratos administrativos vigentes en contratos laborales, siempre que se cumplan los requisitos de cada una de las figuras previstas en esta Ley y no suponga minoración de su dedicación.»

Disposición transitoria quinta. *(Queda sin contenido).*

Disposición adicional primera. *Del Cuerpo de Catedráticos de Escuelas Universitarias y de la integración de sus miembros en el Cuerpo de Profesores Titulares de Universidad.*

A partir de la entrada en vigor de esta Ley, previa solicitud dirigida al Rector de la universidad, los funcionarios y funcionarias Doctores del Cuerpo de Catedráticos de Escuela Universitaria, podrán integrarse en el Cuerpo de Profesores Titulares de Universidad en las mismas plazas que ocupen, manteniendo todos su derechos, y computándose la fecha de ingreso en el Cuerpo de Profesores Titulares de Universidad la que tuvieran en el cuerpo de origen. Quienes no soliciten dicha integración permanecerán en su situación actual y conservarán su plena capacidad docente e investigadora. Asimismo, podrán presentar la solicitud para obtener la acreditación para catedrático de universidad prevista en el artículo 60.1 de esta Ley Orgánica de Universidades.

Disposición adicional segunda. *Del Cuerpo de Profesores Titulares de Escuelas Universitarias y de la integración de sus miembros en el Cuerpo de Profesores Titulares de Universidad.*

1. A los efectos del acceso de estos profesores al Cuerpo de Profesores y Profesoras Titulares de Universidad, los profesores titulares de escuela universitaria que, a la entrada en vigor de esta Ley, posean el título de Doctor o lo obtengan posteriormente, y se acrediten específicamente en el marco de lo previsto por el artículo 57, accederán directamente al Cuerpo de Profesores Titulares de Universidad, en sus propias plazas. Para la acreditación de Profesores Titulares de Escuela Universitaria se valorará la investigación, la gestión y, particularmente, la docencia.

2. Las universidades establecerán programas tendentes a favorecer que los Profesores Titulares de Escuela Universitaria puedan compaginar sus tareas docentes con la obtención del título de Doctor.

3. Quienes no accedan a la condición de Profesor Titular de universidad permanecerán en su situación actual, manteniendo todos sus derechos y conservando su plena capacidad docente y, en su caso, investigadora.

4. Mientras exista profesorado Titular de Escuelas Universitarias o habilitado para dicha categoría que no esté acreditado para una categoría superior, las Universidades podrán convocar concursos entre los mismos para ocupar plazas de Titulares de Escuelas Universitarias.

Disposición adicional tercera. *De los actuales profesores colaboradores.*

Quienes a la entrada en vigor de esta Ley estén contratados como profesoras y profesores colaboradores con arreglo a la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, podrán continuar en el desempeño de sus funciones docentes e investigadoras.

Asimismo, quienes estén contratados como colaboradores con carácter indefinido, posean el título de Doctor o lo obtengan tras la entrada en vigor de esta Ley y reciban la evaluación positiva a que se refiere el apartado a) del artículo 52, accederán directamente a la categoría de Profesora o Profesor Contratado Doctor, en sus propias plazas.

Disposición adicional cuarta. *Programas específicos de ayuda.*

Las Administraciones públicas competentes, en coordinación con las respectivas universidades, establecerán programas específicos para que las víctimas del terrorismo y de la violencia de género, así como las personas con discapacidad, puedan recibir la ayuda personalizada, los apoyos y las adaptaciones en el régimen docente.

Disposición adicional quinta. *Referencias.*

Todas las referencias que la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, hace al Ministerio de Educación, Cultura y Deporte se entenderán sustituidas por la referencia al «ministerio competente en materia de universidades». Asimismo, las referencias realizadas al Consejo de Coordinación Universitaria en los artículos 2.5, 4, 43.1, 44, 68.1, 81.3.b) y 85.1 y en las disposiciones adicionales séptima y octava de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, se entenderán realizadas a la Conferencia General de Política Universitaria, y las realizadas en los artículos 46.3, 71.2, 86.1 y en la disposición adicional vigésima quinta de la misma Ley se entenderán realizadas al Consejo de Universidades.

Disposición adicional sexta. *Estatuto del personal docente o investigador.*

El Gobierno, en el plazo de un año desde la entrada en vigor de esta Ley, aprobará mediante Real Decreto el estatuto del personal docente o investigador universitario, que incluirá la regulación de una estructura de carrera funcionarial que esté basada en la obtención de méritos docentes o investigadores, así como las condiciones en las que los

profesores o investigadores funcionarios universitarios podrán participar en la gestión y explotación de los resultados de su investigación.

Disposición adicional séptima. *Elaboración de planes destinados a personas con necesidades especiales.*

Las universidades, en el plazo de un año desde la entrada en vigor de esta Ley, y previa consulta de las organizaciones representativas de los respectivos sectores sociales concernidos, elaborarán los planes que den cumplimiento al mandato previsto en la disposición adicional vigésima cuarta de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, en la redacción dada por esta Ley.

Disposición adicional octava. *Adaptación de estatutos.*

Las universidades adaptarán sus estatutos conforme a lo dispuesto en la presente Ley en un plazo máximo de tres años.

Hasta tanto se produzca la adaptación de los estatutos, los Consejos de Gobierno de las universidades podrán aprobar la normativa de aplicación que sea necesaria para el cumplimiento de lo establecido en esta Ley.

Disposición adicional novena. *Adaptación de las universidades privadas.*

1. Las universidades privadas y centros universitarios adscritos deberán adaptar sus normas de organización y funcionamiento a las previsiones de esta Ley que les afecten en el plazo de tres años desde su entrada en vigor.

2. Las universidades privadas deberán alcanzar el porcentaje del 50 por ciento y el 60 por ciento a los que se refiere el artículo 72.2 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, modificada por esta Ley, en el plazo máximo de seis años contado desde la fecha de entrada en vigor de esta Ley.

3. El profesorado de los centros privados de enseñanza universitaria adscritos a universidades públicas y el de las universidades no presenciales financiadas mayoritariamente por Administraciones públicas deberá adaptarse a lo establecido por el artículo 72 de esta Ley en el plazo máximo de cuatro años desde su entrada en vigor.

Disposición adicional décima. *De los habilitados.*

Quienes resultaran habilitados o habilitadas conforme a la regulación correspondiente contenida en la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, y su normativa de desarrollo se entenderá que poseen la acreditación regulada en la reforma de dicha ley orgánica realizada por esta Ley.

Se entenderá que los habilitados para Catedrático de Escuela Universitaria lo están para Profesor Titular de Universidad.

Disposición adicional undécima. *Reconocimiento de efectos civiles.*

El Gobierno, a propuesta de los ministerios competentes en materia de justicia y universidades, en aplicación de lo establecido en los Acuerdos de Cooperación entre el Estado y la Federación de Entidades Religiosas Evangélicas de España, aprobado por la Ley 24/1992, de 10 de noviembre, la Federación de Comunidades Israelitas de España, aprobado por la Ley 25/1992, de 10 de noviembre, y la Comisión Islámica de España, aprobado por la Ley 26/1992, de 10 de noviembre, regulará las condiciones para el reconocimiento de efectos civiles de los títulos académicos relativos a enseñanzas, de nivel universitario, de carácter teológico y de formación de ministros de culto, impartidas en centros docentes de nivel superior dependientes de las mencionadas entidades religiosas.

Lo anterior será extensible al caso de otros acuerdos de cooperación que se concluyan en el futuro, siempre que en ellos se recoja esta posibilidad.

Disposición adicional duodécima. *Unidades de igualdad.*

Las universidades contarán entre sus estructuras de organización con unidades de igualdad para el desarrollo de las funciones relacionadas con el principio de igualdad entre mujeres y hombres.

Disposición adicional decimotercera. *Tratamientos.*

Las autoridades universitarias recibirán el tratamiento de señor o señora, seguido de la denominación del cargo. Los Rectores de las universidades recibirán, además, el tratamiento académico de Rector Magnífico o Rectora Magnífica.

Disposición adicional decimocuarta. *Estatuto del estudiante universitario.*

En el plazo de un año desde la entrada en vigor de esta Ley, el Gobierno aprobará el Estatuto del estudiante universitario previsto en el artículo 46.5 de la Ley Orgánica 6/2001, de 21 de diciembre, en la redacción dada por esta Ley.

Disposición adicional decimoquinta. *Derechos adquiridos.*

Los títulos universitarios de Diplomado Universitario, Arquitecto Técnico, Ingeniero Técnico, Licenciado, Arquitecto e Ingeniero mantendrán su plena vigencia académica y profesional en los mismos términos en que se establecieron.

Disposición adicional decimosexta. *Proyección exterior de las universidades.*

(Derogada)

Disposición adicional decimoséptima. *De los profesores estables o permanentes de los centros de titularidad pública de enseñanza superior (INEF), creados con anterioridad a la incorporación a la universidad de los estudios conducentes al título oficial en Ciencias de la Actividad Física y del Deporte.*

1. A los efectos del acceso de estos profesores al Cuerpo de Profesores Titulares de Universidad, los profesores funcionarios numerarios de la Escala de Profesores del INEF de Galicia (Administración General, grupo A) de la Xunta de Galicia que, a la entrada en vigor de esta Ley, posean el título de doctor o que lo obtengan tras su entrada en vigor y se acrediten específicamente en el marco de lo previsto por el artículo 57, accederán directamente al Cuerpo de Profesores Titulares de Universidad, en sus propias plazas de la Universidad de A Coruña. Para la acreditación de los Profesores funcionarios numerarios de la Escala de profesores del INEF de Galicia (Administración General, grupo A) de la Xunta de Galicia, se valorará la investigación, la gestión y, particularmente, la docencia.

Quienes no accedan a la condición de profesor titular de universidad permanecerán en su situación actual, manteniendo todos los derechos y conservando su plena capacidad docente y, en su caso, investigadora.

2. A los efectos del acceso de los profesores del INEF de Cataluña al cuerpo de profesores titulares de Universidad, los profesores que a la entrada en vigor de esta Ley sean profesores estables o permanentes en las plantillas del INEFC y que en el momento de la integración de los centros del INEFC en las respectivas universidades sean funcionarios del Grupo A de la Generalitat de Cataluña en los cuerpos correspondientes, y además posean el título de doctor, o que lo obtengan tras su entrada en vigor, y se acrediten específicamente en el marco de lo previsto por el artículo 57, accederán directamente al Cuerpo de Profesores Titulares de Universidad, en las plazas correspondientes en la Universidad a la que cada uno de los Centros se hubiera integrado. Para la acreditación específica de los profesores a los que se refiere este apartado se valorará la investigación, la gestión y, particularmente, la docencia.

Quienes no accedan a la condición de profesor titular de universidad permanecerán en su situación actual, manteniendo todos los derechos y conservando su plena capacidad docente y, en su caso, investigadora.

3. A los efectos del acceso de los profesores estables o fijos del INEF de Madrid que permanecen en sus plazas de la Comunidad Autónoma de Madrid al Cuerpo de Profesores Titulares de Universidad, y que a la entrada en vigor de esta Ley sean funcionarios del Grupo A de la Comunidad de Madrid en los cuerpos correspondientes, y además posean el título de doctor, o que lo obtengan tras su entrada en vigor, y se acrediten específicamente en el marco de lo previsto por el artículo 57, accederán directamente al Cuerpo de Profesores Titulares de Universidad, en las plazas correspondientes de la Universidad Politécnica de Madrid, donde ya fue integrado el Centro. Para la acreditación específica de los profesores a los que se refiere este apartado se valorará la investigación, la gestión y, particularmente, la docencia.

Quienes no accedan a la condición de profesor titular de universidad permanecerán en su situación actual, manteniendo todos sus derechos y conservando su plena capacidad docente y, en su caso, investigadora.

4. A los efectos del acceso de los profesores del INEF de Andalucía y del IVEF del País Vasco que permanecen en sus plazas ya transferidas respectivamente a las universidades de Granada y del País Vasco, y que posean el título de doctor, o que lo obtengan tras la entrada en vigor de la presente Ley, podrán solicitar acreditarse específicamente en el marco de lo previsto por el artículo 57. Para la acreditación específica de los profesores a los que se refiere este apartado se valorará la investigación, la gestión y, particularmente, la docencia.

Quienes no accedan a la condición de profesor titular de universidad permanecerán en su situación actual, manteniendo todos sus derechos y conservando su plena capacidad docente y, en su caso, investigadora.

5. Quienes, perteneciendo al Cuerpo de Profesores Titulares de Universidad, hubiesen obtenido una plaza de carácter estable o permanente en la plantilla de alguno de los centros citados en esta Disposición adicional con anterioridad a la incorporación de los estudios universitarios conducentes al título oficial de Licenciado en Ciencias de la Actividad Física y del Deporte al catálogo de títulos universitarios oficiales, y posean el título de Doctor a la entrada en vigor de esta Ley, y quienes a la entrada en vigor de esta Ley tengan la categoría de catedrático del INEF de Cataluña, podrán presentar solicitud para obtener la acreditación prevista en el artículo 60 de la presente Ley, para acceder al Cuerpo de Catedráticos de Universidad.

Quienes no soliciten dicha integración permanecerán en su situación actual y conservarán su plena capacidad docente e investigadora.

Disposición adicional decimoctava. *Deducción por donaciones a universidades públicas y privadas de entidades sin fines lucrativos.*

1. Los porcentajes de deducción y del límite de la base de deducción establecidos en los artículos 19, 20 y 21 de la Ley 49/2002, de 23 de diciembre, de régimen fiscal de las entidades sin fines lucrativos y de los incentivos fiscales al mecenazgo, se elevarán en cinco puntos porcentuales por los donativos y donaciones establecidos en el artículo 17 de la Ley 49/2002 realizados a favor de universidades públicas y privadas de entidades sin fines lucrativos a las que se refiere el artículo 2 de la Ley 49/2002, que hayan comunicado la opción por aplicar el régimen fiscal especial, siempre que esas universidades desarrollen enseñanzas de doctorado o tercer ciclo de estudios universitarios.

2. Dichas universidades deberán destinar el importe del donativo o el bien o derecho donado a programas de investigación universitaria y doctorado, debiendo constar en la certificación que han de expedir en los términos establecidos en el artículo 24 de la Ley 49/2002.

Disposición adicional decimonovena. *Compensación de precios públicos.*

Cualquier reducción de tasas universitarias regulada por la Administración competente será compensada anualmente en los presupuestos de la universidad mediante transferencias.

Disposición adicional vigésima. *De los profesores numerarios de Escuelas Oficiales de Náutica.*

Los funcionarios del Cuerpo de Profesores Numerarios de Escuelas Oficiales de Náutica no integrados en el Cuerpo de Profesores Titulares de Universidad les será de aplicación lo dispuesto en la disposición adicional segunda.

Disposición adicional vigésima primera. *Protección de datos de carácter personal.*

1. Lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, será de aplicación al tratamiento y cesión de datos derivados de lo dispuesto en esta Ley Orgánica.

Las universidades deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, tratamiento o acceso no autorizados.

2. El Gobierno regulará, previo informe de la Agencia Española de Protección de Datos, el contenido de los currículos a los que se refieren los artículos 57.2 y 62.3.

3. No será preciso el consentimiento de los estudiantes para la publicación de los resultados de las pruebas relacionadas con la evaluación de sus conocimientos y competencias ni de los actos que resulten necesarios para la adecuada realización y seguimiento de dicha evaluación.

4. Igualmente no será preciso el consentimiento del personal de las universidades para la publicación de los resultados de los procesos de evaluación de su actividad docente, investigadora y de gestión realizados por la universidad o por las agencias o instituciones públicas de evaluación.

5. El Gobierno regulará, previo informe de la Agencia Española de Protección de Datos, el contenido académico y científico de los currículos de los profesores e investigadores que las universidades y las agencias o instituciones públicas de evaluación académica y científica pueden hacer público, no siendo preciso en este caso el consentimiento previo de los profesores o investigadores.

Disposición adicional vigésima segunda. *Del Observatorio de becas y ayudas al estudio.*

El Gobierno, previo acuerdo de la Conferencia General de Política Universitaria y del Consejo de Universidades, establecerá un Observatorio de becas y ayudas al estudio. El Observatorio elaborará estadísticas e informes que contribuyan a mejorar la eficiencia y transparencia del sistema de becas y ayudas universitarias. En su funcionamiento se contará con la participación de los agentes sociales y de los estudiantes.

Disposición adicional vigésima tercera. *Jubilación voluntaria anticipada.*

El Gobierno, las Comunidades Autónomas y las Universidades promoverán, en el marco del estudio que el Gobierno realice y envíe al Congreso de los Diputados sobre el acceso a la jubilación voluntaria anticipada de determinados colectivos, el establecimiento de acuerdos que faciliten la reducción paulatina de actividad, una vez alcanzados los sesenta años, y la jubilación voluntaria anticipada del personal de las universidades. El Estatuto del Personal Docente e Investigador previsto en la disposición adicional sexta desarrollará la jubilación voluntaria.

Disposición adicional vigésima cuarta. *Modificación de la Ley 53/1984, de 26 de diciembre, de incompatibilidades del personal al servicio de las Administraciones públicas.*

Las limitaciones establecidas en el artículo 12.1 b) y d) de la Ley 53/1984, de 26 de diciembre, de incompatibilidades del personal al servicio de las Administraciones públicas, no serán de aplicación a los profesores y profesoras funcionarios de los cuerpos docentes universitarios cuando participen en empresas de base tecnológica, promovidas por su universidad y participadas por ésta o por alguno de los entes previstos en el artículo 84 de esta Ley, creadas a partir de patentes o de resultados generados por proyectos de investigación realizados en universidades, siempre que exista un acuerdo explícito del

Consejo de Gobierno de la Universidad, previo informe del Consejo Social, que permita la creación de dicha empresa.

En este acuerdo se debe certificar la naturaleza de base tecnológica de la empresa, y las contraprestaciones adecuadas a favor de la universidad. El Gobierno regulará las condiciones para la determinación de la naturaleza de base tecnológica de las empresas a las que se refiere el párrafo anterior.

Disposición transitoria primera. *Sustitución del sistema de habilitación.*

Hasta un año después de la resolución de las últimas pruebas de habilitación convocadas, las universidades podrán decidir la convocatoria de plazas para los Cuerpos de Catedráticos de Universidad y de Profesores Titulares de Universidad mediante concurso de acceso entre habilitados comunicándolo a la Secretaría General del Consejo de Coordinación Universitaria, todo ello según lo dispuesto en el artículo 62 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, y su normativa de desarrollo, que, a estos efectos, se considerará vigente.

Disposición transitoria segunda. *Contratación de profesores colaboradores.*

El Gobierno, previo informe del Consejo de Universidades, establecerá reglamentariamente las condiciones y plazos en los que, de forma excepcional, las universidades podrán contratar profesores colaboradores entre diplomados, arquitectos técnicos o ingenieros técnicos que, en todo caso, deberán contar con informe favorable de la Agencia Nacional de Evaluación de la Calidad y la Acreditación o del órgano de evaluación externa que la Ley de la Comunidad Autónoma determine.

Disposición transitoria tercera. *Extinción de las enseñanzas anteriores.*

Hasta tanto el Gobierno determine las condiciones y la fecha de la definitiva extinción de las enseñanzas conducentes a la obtención de los títulos oficiales de la ordenación universitaria anterior, las universidades podrán seguir impartiendo dichas enseñanzas de acuerdo con su normativa aplicable.

Disposición final primera. *Modificación de la Ley 14/1986, de 25 de abril, General de Sanidad.*

El artículo 105 de la Ley 14/1986, de 25 de abril, General de Sanidad, queda redactado del siguiente modo:

> **«Artículo 105.**
>
> 1. En el marco de la planificación asistencial y docente de las Administraciones públicas, el régimen de conciertos entre las universidades y las instituciones sanitarias podrá establecer la vinculación de determinadas plazas asistenciales de la institución sanitaria con plazas docentes de los cuerpos de profesores de universidad y con plazas de profesor contratado doctor.
>
> Las plazas así vinculadas se proveerán por concurso entre quienes hayan sido seleccionados en los concursos de acceso a los cuerpos de funcionarios docentes universitarios o a plazas de profesor contratado doctor, conforme a las normas que les son propias.
>
> Quienes participen en los procesos de acreditación nacional, previos a los mencionados concursos, además de reunir los requisitos exigidos en las indicadas normas, acreditarán estar en posesión del título de Especialista en Ciencias de la Salud que proceda y cumplir las exigencias que, en cuanto a su cualificación asistencial, se determinen reglamentariamente. Asimismo, las comisiones deberán valorar los méritos e historial académico e investigador y los propios de la labor asistencial de los candidatos y candidatas, en la forma que reglamentariamente se establezca.

En las comisiones que resuelvan los mencionados concursos de acceso, dos de sus miembros serán elegidos por sorteo público por la institución sanitaria correspondiente.

2. Los conciertos podrán establecer, asimismo, un número de plazas de profesores asociados que deberá cubrirse por personal asistencial que esté prestando servicios en la institución sanitaria concertada. Este número no será tenido en cuenta a los efectos del porcentaje de contratados que rige para las universidades públicas. Estos profesores asociados se regirán por las normas propias de los profesores asociados de la universidad, con las peculiaridades que reglamentariamente se establezcan en cuanto al régimen temporal de sus contratos. Los estatutos de la universidad deberán recoger fórmulas específicas para regular la participación de estos profesores y profesoras en los órganos de gobierno de la universidad.

3. Los conciertos establecerán, asimismo, el número de plazas de ayudante, profesor ayudante doctor y profesor contratado doctor, en las relaciones de puestos de trabajo de las universidades públicas, que deberán cubrirse mediante concursos públicos entre profesionales sanitarios que hubieran obtenido el título de especialista en los tres años anteriores a la convocatoria del concurso.»

Disposición final segunda. *Modificación de la Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesiones Sanitarias.*

El párrafo a) del apartado 3 del artículo 20 de la Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesiones Sanitarias, queda redactado del siguiente modo:

«a) Los residentes realizarán el programa formativo de la especialidad con dedicación a tiempo completo. La formación mediante residencia será incompatible con cualquier otra actividad profesional. También será incompatible con cualquier actividad formativa, siempre que ésta se desarrolle dentro de la jornada laboral de la relación laboral especial del residente.»

Disposición final tercera. *Modificación de la Ley 13/1986, de 14 de abril, de fomento y coordinación general de la investigación científica y técnica.*

1. Se añade al párrafo quinto de la letra b) del apartado 1 del artículo 17 de la Ley 13/1986, de 14 de abril, de fomento y coordinación general de la investigación científica y técnica, la siguiente frase:

«Las situaciones de incapacidad temporal, maternidad y adopción o acogimiento durante el período de duración del contrato, interrumpirán su cómputo.»

2. Se añade al artículo 17 de la Ley 13/1986, de 14 de abril, de fomento y coordinación general de la investigación científica y técnica, un apartado 3 con la siguiente redacción:

«3. Sin perjuicio de lo previsto en los apartados anteriores, las Universidades Públicas, las Agencias Estatales de Investigación y los centros públicos de investigación no estatales, así como las instituciones sin ánimo de lucro que realicen actividades de investigación y desarrollo tecnológico podrán, previa convocatoria pública, garantizando los principios de igualdad, mérito y capacidad, conforme a la legislación aplicable y a sus normas de organización y funcionamiento, y en función de sus necesidades de personal y de acuerdo con sus disponibilidades presupuestarias celebrar contratos con carácter indefinido y dedicación a tiempo completo, con los investigadores que hayan sido contratados conforme a las previsiones de la letra b) del apartado 1 y que en el desarrollo de su actividad hayan superado con criterios de excelencia la evaluación correspondiente. La finalidad del contrato será realizar las funciones de la institución y prioritariamente tareas de investigación científica y desarrollo tecnológico.»

Disposición final cuarta. *Modificación del Real Decreto Legislativo 2/2004, de 5 de marzo, que aprueba el texto refundido de la Ley Reguladora de las Haciendas Locales.*

Se adiciona un nuevo apartado 2 bis) al artículo 74 de la Ley Reguladora de las Haciendas Locales, con el siguiente redactado:

> «2 bis) Los ayuntamientos mediante ordenanza podrán regular una bonificación de hasta el 95 por ciento de la cuota íntegra del impuesto a favor de inmuebles de organismos públicos de investigación y los de enseñanza universitaria.»

Disposición final quinta. *Procedimiento para evaluar el impacto de diversas medidas establecidas por la presente Ley.*

Dos años después de la entrada en vigor de la presente Ley, el Gobierno presentará en el Congreso de los Diputados un estudio para evaluar el impacto de las modificaciones incorporadas por la presente Ley en relación a:

1. El otorgamiento de excedencias de profesoras y profesores funcionarios de cuerpos docentes universitarios para incorporarse a empresas de base tecnológica, a las que se refiere el artículo 83 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.
2. Participación de profesoras y profesores funcionarios de los cuerpos docentes universitarios en empresas de base tecnológica de acuerdo con lo que establece la disposición adicional vigésimo cuarta de la presente Ley.

Disposición final sexta. *Título competencial.*

Esta Ley se dicta al amparo de las competencias que corresponden al Estado conforme al artículo 149.1.1.ª, 15.ª, 18.ª y 30.ª de la Constitución.

Disposición final séptima. *Habilitación para el desarrollo reglamentario.*

1. Corresponde al Gobierno y a las Comunidades Autónomas, en el ámbito de sus respectivas competencias, dictar las disposiciones necesarias para el desarrollo y la aplicación de esta Ley.
2. En el plazo máximo de cuatro meses desde la entrada en vigor de esta Ley, el Gobierno aprobará el reglamento por el que se regula la práctica de la acreditación y los concursos de acceso regulados en los artículos 57 y siguientes de la Ley Orgánica 6/2001, de 21 de diciembre, en la redacción efectuada por esta Ley.

Disposición final octava. *Carácter de ley orgánica.*

Tienen el carácter de ley orgánica los apartados ocho, veinticinco, treinta, treinta y uno, treinta y dos, treinta y cuatro, treinta y cinco, treinta y siete, treinta y ocho, cuarenta y tres, cuarenta y cinco, cuarenta y seis, cuarenta y siete, setenta y cuatro, setenta y cinco, los artículos 87 y 88 del apartado ochenta y uno, el ochenta y seis, el noventa y el noventa y uno del artículo único, así como las disposiciones adicionales novena y vigésimo primera y esta disposición final. Los demás preceptos no tienen carácter orgánico.

§ 54

Ley Orgánica 2/2006, de 3 de mayo, de Educación. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 106, de 4 de mayo de 2006
Última modificación: 23 de marzo de 2018
Referencia: BOE-A-2006-7899

Téngase en cuenta, el calendario de implantación regulado en la disposición final 5, para las modificaciones introducidas por la Ley Orgánica 8/2013, de 9 de diciembre. Ref. BOE-A-2013-12886. en la redacción dada por el art. 1 del Real Decreto-ley 5/2016, de 9 de diciembre. Ref. BOE-A-2016-11733
Véanse los arts. 2, 3 y 4 del citado Real Decreto-ley 5/2016, en cuanto a la adecuación del régimen jurídico de la evaluación final al nuevo calendario de implantación.

[. . .]

Disposición adicional vigesimotercera. *Datos personales de los alumnos.*

1. Los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichos datos podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos.

2. Los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo. La incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos. En todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.

3. En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad. El profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo.

4. La cesión de los datos, incluidos los de carácter reservado, necesarios para el sistema educativo, se realizará preferentemente por vía telemática y estará sujeta a la legislación en materia de protección de datos de carácter personal. En el caso de la cesión de datos entre Comunidades Autónomas o entre éstas y el Estado, las condiciones mínimas serán

acordadas por el Gobierno con las Comunidades Autónomas, en el seno de la Conferencia Sectorial de Educación.

[. . .]

§ 55

Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 313, de 29 de diciembre de 2004
Última modificación: 4 de agosto de 2018
Referencia: BOE-A-2004-21760

[. . .]

TÍTULO V

Tutela Judicial

[. . .]

CAPÍTULO IV

Medidas judiciales de protección y de seguridad de las víctimas

[. . .]

Artículo 63. *De la protección de datos y las limitaciones a la publicidad.*

1. En las actuaciones y procedimientos relacionados con la violencia de género se protegerá la intimidad de las víctimas; en especial, sus datos personales, los de sus descendientes y los de cualquier otra persona que esté bajo su guarda o custodia.

2. Los Jueces competentes podrán acordar, de oficio o a instancia de parte, que las vistas se desarrollen a puerta cerrada y que las actuaciones sean reservadas.

[. . .]

§ 56

Ley 59/2003, de 19 de diciembre, de firma electrónica. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 304, de 20 de diciembre de 2003
Última modificación: 2 de octubre de 2015
Referencia: BOE-A-2003-23399

[. . .]

TÍTULO III

Prestación de servicios de certificación

CAPÍTULO I

Obligaciones

Artículo 17. *Protección de los datos personales.*

1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta ley se sujetará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en sus normas de desarrollo.

2. Para la expedición de certificados electrónicos al público, los prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos.

Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de otros servicios en relación con la firma electrónica, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante.

3. Los prestadores de servicios de certificación que consignen un seudónimo en el certificado electrónico a solicitud del firmante deberán constatar su verdadera identidad y conservar la documentación que la acredite.

Dichos prestadores de servicios de certificación estarán obligados a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica de Protección de Datos de Carácter Personal en que así se requiera.

4. En cualquier caso, los prestadores de servicios de certificación no incluirán en los certificados electrónicos que expidan, los datos a los que se hace referencia en el artículo 7

de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[. . .]

Artículo 19. *Declaración de prácticas de certificación.*

1. Todos los prestadores de servicios de certificación formularán una declaración de prácticas de certificación en la que detallarán, en el marco de esta ley y de sus disposiciones de desarrollo, las obligaciones que se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

2. La declaración de prácticas de certificación de cada prestador estará disponible al público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita.

3. La declaración de prácticas de certificación tendrá la consideración de documento de seguridad a los efectos previstos en la legislación en materia de protección de datos de carácter personal y deberá contener todos los requisitos exigidos para dicho documento en la mencionada legislación.

[. . .]

TÍTULO VI

Infracciones y sanciones

Artículo 31. *Infracciones.*

1. Las infracciones de los preceptos de esta ley se clasifican en muy graves, graves y leves.

2. Son infracciones muy graves:

a) El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, siempre que se hayan causado daños graves a los usuarios o la seguridad de los servicios de certificación se haya visto gravemente afectada.

Lo dispuesto en este apartado no será de aplicación respecto al incumplimiento de la obligación de constitución de la garantía económica prevista en el apartado 2 del artículo 20.

b) La expedición de certificados reconocidos sin realizar todas las comprobaciones previas señaladas en el artículo 12, cuando ello afecte a la mayoría de los certificados reconocidos expedidos en los tres años anteriores al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este período es menor.

3. Son infracciones graves:

a) El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, excepto de la obligación de constitución de la garantía prevista en el apartado 2 del artículo 20, cuando no constituya infracción muy grave.

b) La falta de constitución por los prestadores que expidan certificados reconocidos de la garantía económica contemplada en el apartado 2 del artículo 20.

c) La expedición de certificados reconocidos sin realizar todas las comprobaciones previas indicadas en el artículo 12, en los casos en que no constituya infracción muy grave.

d) El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones señaladas en el artículo 18, si se hubieran causado daños graves a los usuarios o la seguridad de los servicios de certificación se hubiera visto gravemente afectada.

e) El incumplimiento por los prestadores de servicios de certificación de las obligaciones establecidas en el artículo 21 respecto al cese de actividad de los mismos o la producción de circunstancias que impidan la continuación de su actividad, cuando las mismas no sean sancionables de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

f) La resistencia, obstrucción, excusa o negativa injustificada a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta ley y la falta o deficiente presentación de la información solicitada por parte del Ministerio de Ciencia y Tecnología en su función de inspección y control.

g) El incumplimiento de las resoluciones dictadas por el Ministerio de Ciencia y Tecnología para asegurar que el prestador de servicios de certificación se ajuste a esta ley.

4. Constituyen infracciones leves:

El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones establecidas en el artículo 18; y el incumplimiento por los prestadores de servicios de certificación de las restantes obligaciones establecidas en esta Ley, cuando no constituya infracción grave o muy grave, con excepción de las obligaciones contenidas en el apartado 2 del artículo 30.

[. . .]

Artículo 36. *Competencia y procedimiento sancionador.*

1. La imposición de sanciones por el incumplimiento de lo previsto en esta ley corresponderá, en el caso de infracciones muy graves, al Ministro de Ciencia y Tecnología y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

No obstante, el incumplimiento de las obligaciones establecidas en el artículo 17 será sancionado por la Agencia de Protección de Datos con arreglo a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en sus normas de desarrollo.

[. . .]

§ 57

Ley 58/2003, de 17 de diciembre, General Tributaria. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 302, de 18 de diciembre de 2003
Última modificación: 4 de julio de 2018
Referencia: BOE-A-2003-23186

[. . .]

TÍTULO III

La aplicación de los tributos

CAPÍTULO I

Principios generales

[. . .]

Sección 3.ª Colaboración social en la aplicación de los tributos

[. . .]

Artículo 94. *Autoridades sometidas al deber de informar y colaborar.*

1. Las autoridades, cualquiera que sea su naturaleza, los titulares de los órganos del Estado, de las comunidades autónomas y de las entidades locales; los organismos autónomos y las entidades públicas empresariales; las cámaras y corporaciones, colegios y asociaciones profesionales; las mutualidades de previsión social; las demás entidades públicas, incluidas las gestoras de la Seguridad Social y quienes, en general, ejerzan funciones públicas, estarán obligados a suministrar a la Administración tributaria cuantos datos, informes y antecedentes con trascendencia tributaria recabe ésta mediante disposiciones de carácter general o a través de requerimientos concretos, y a prestarle, a ella y a sus agentes, apoyo, concurso, auxilio y protección para el ejercicio de sus funciones.

Asimismo, participarán en la gestión o exacción de los tributos mediante las advertencias, repercusiones y retenciones, documentales o pecuniarias, de acuerdo con lo previsto en las leyes o disposiciones reglamentarias vigentes.

2. A las mismas obligaciones quedarán sujetos los partidos políticos, sindicatos y asociaciones empresariales.

3. Los juzgados y tribunales deberán facilitar a la Administración tributaria, de oficio o a requerimiento de la misma, cuantos datos con trascendencia tributaria se desprendan de las actuaciones judiciales de las que conozcan, respetando, en su caso, el secreto de las diligencias sumariales.

4. El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo, así como la Secretaría de ambas comisiones, facilitarán a la Administración tributaria cuantos datos con trascendencia tributaria obtengan en el ejercicio de sus funciones, de oficio, con carácter general o mediante requerimiento individualizado en los términos que reglamentariamente se establezcan.

Los órganos de la Administración tributaria podrán utilizar la información suministrada para la regularización de la situación tributaria de los obligados en el curso del procedimiento de comprobación o de inspección, sin que sea necesario efectuar el requerimiento al que se refiere el apartado 3 del artículo anterior.

5. La cesión de datos de carácter personal que se deba efectuar a la Administración tributaria conforme a lo dispuesto en el artículo anterior, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito no será de aplicación lo dispuesto en el apartado 1 del artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Artículo 95. *Carácter reservado de los datos con trascendencia tributaria.*

1. Los datos, informes o antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones tienen carácter reservado y sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada y para la imposición de las sanciones que procedan, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión tenga por objeto:

a) La colaboración con los órganos jurisdiccionales y el Ministerio Fiscal en la investigación o persecución de delitos que no sean perseguibles únicamente a instancia de persona agraviada.

b) La colaboración con otras Administraciones tributarias a efectos del cumplimiento de obligaciones fiscales en el ámbito de sus competencias.

c) La colaboración con la Inspección de Trabajo y Seguridad Social y con las entidades gestoras y servicios comunes de la Seguridad Social en la lucha contra el fraude en la cotización y recaudación de las cuotas del sistema de Seguridad Social y contra el fraude en la obtención y disfrute de las prestaciones a cargo del sistema; así como para la determinación del nivel de aportación de cada usuario en las prestaciones del Sistema Nacional de Salud.

d) La colaboración con las Administraciones públicas para la lucha contra el delito fiscal y contra el fraude en la obtención o percepción de ayudas o subvenciones a cargo de fondos públicos o de la Unión Europea.

e) La colaboración con las comisiones parlamentarias de investigación en el marco legalmente establecido.

f) La protección de los derechos e intereses de los menores e incapacitados por los órganos jurisdiccionales o el Ministerio Fiscal.

g) La colaboración con el Tribunal de Cuentas en el ejercicio de sus funciones de fiscalización de la Agencia Estatal de Administración Tributaria.

h) La colaboración con los jueces y tribunales para la ejecución de resoluciones judiciales firmes. La solicitud judicial de información exigirá resolución expresa en la que, previa ponderación de los intereses públicos y privados afectados en el asunto de que se trate y por haberse agotado los demás medios o fuentes de conocimiento sobre la existencia de bienes y derechos del deudor, se motive la necesidad de recabar datos de la Administración tributaria.

i) La colaboración con el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, con la Comisión de Vigilancia de Actividades de Financiación del Terrorismo y con la Secretaría de ambas comisiones, en el ejercicio de sus funciones respectivas.

j) La colaboración con órganos o entidades de derecho público encargados de la recaudación de recursos públicos no tributarios para la correcta identificación de los obligados al pago y con la Dirección General de Tráfico para la práctica de las notificaciones a los mismos, dirigidas al cobro de tales recursos.

k) La colaboración con las Administraciones públicas para el desarrollo de sus funciones, previa autorización de los obligados tributarios a que se refieran los datos suministrados.

l) La colaboración con la Intervención General de la Administración del Estado en el ejercicio de sus funciones de control de la gestión económico-financiera, el seguimiento del déficit público, el control de subvenciones y ayudas públicas y la lucha contra la morosidad en las operaciones comerciales de las entidades del Sector Público.

m) La colaboración con la Oficina de Recuperación y Gestión de Activos mediante la cesión de los datos, informes o antecedentes necesarios para la localización de los bienes embargados o decomisados en un proceso penal, previa acreditación de esta circunstancia.

2. En los casos de cesión previstos en el apartado anterior, la información de carácter tributario deberá ser suministrada preferentemente mediante la utilización de medios informáticos o telemáticos. Cuando las Administraciones públicas puedan disponer de la información por dichos medios, no podrán exigir a los interesados la aportación de certificados de la Administración tributaria en relación con dicha información.

3. La Administración tributaria adoptará las medidas necesarias para garantizar la confidencialidad de la información tributaria y su uso adecuado.

Cuantas autoridades o funcionarios tengan conocimiento de estos datos, informes o antecedentes estarán obligados al más estricto y completo sigilo respecto de ellos, salvo en los casos citados. Con independencia de las responsabilidades penales o civiles que pudieran derivarse, la infracción de este particular deber de sigilo se considerará siempre falta disciplinaria muy grave.

Cuando se aprecie la posible existencia de un delito no perseguible únicamente a instancia de persona agraviada, la Administración tributaria deducirá el tanto de culpa o remitirá al Ministerio Fiscal relación circunstanciada de los hechos que se estimen constitutivos de delito. También podrá iniciarse directamente el oportuno procedimiento mediante querella a través del Servicio Jurídico competente.

4. El carácter reservado de los datos establecido en este artículo no impedirá la publicidad de los mismos cuando ésta se derive de la normativa de la Unión Europea.

5. Los retenedores y obligados a realizar ingresos a cuenta sólo podrán utilizar los datos, informes o antecedentes relativos a otros obligados tributarios para el correcto cumplimiento y efectiva aplicación de la obligación de realizar pagos a cuenta. Dichos datos deberán ser comunicados a la Administración tributaria en los casos previstos en la normativa propia de cada tributo.

Salvo lo dispuesto en el párrafo anterior, los referidos datos, informes o antecedentes tienen carácter reservado. Los retenedores y obligados a realizar ingresos a cuenta quedan sujetos al más estricto y completo sigilo respecto de ellos.

6. La cesión de información en el ámbito de la asistencia mutua se regirá por lo dispuesto en el artículo 177 ter de esta Ley.

Artículo 95 bis. *Publicidad de situaciones de incumplimiento relevante de las obligaciones tributarias.*

1. La Administración Tributaria acordará la publicación periódica de listados comprensivos de deudores a la Hacienda Pública por deudas o sanciones tributarias cuando concurran las siguientes circunstancias:

a) Que el importe total de las deudas y sanciones tributarias pendientes de ingreso supere el importe de 1.000.000 de euros.

b) Que dichas deudas o sanciones tributarias no hubiesen sido pagadas transcurrido el plazo de ingreso en periodo voluntario.

A efectos de lo dispuesto en este artículo no se incluirán aquellas deudas y sanciones tributarias que se encuentren aplazadas o suspendidas.

2. En dichos listados se incluirá la siguiente información:

a) La identificación de los deudores conforme al siguiente detalle:

– Personas Físicas: nombre apellidos y NIF.
– Personas Jurídicas y entidades del artículo 35.4 de esta Ley: razón o denominación social completa y NIF.

b) El importe conjunto de las deudas y sanciones pendientes de pago tenidas en cuenta a efectos de la publicación.

3. En el ámbito del Estado, la publicidad regulada en este artículo se referirá exclusivamente a los tributos de titularidad estatal para los que la aplicación de los tributos, el ejercicio de la potestad sancionadora y las facultades de revisión estén atribuidas en exclusiva a los órganos de la Administración Tributaria del Estado no habiendo existido delegación alguna de competencias en estos ámbitos a favor de las Comunidades Autónomas o Entes Locales.

La publicidad regulada en este artículo resultará de aplicación respecto a los tributos que integran la deuda aduanera.

4. La determinación de la concurrencia de los requisitos exigidos para la inclusión en el listado tomará como fecha de referencia el 31 de diciembre del año anterior al del acuerdo de publicación, cualquiera que sea la cantidad pendiente de ingreso a la fecha de dicho acuerdo.

La propuesta de inclusión en el listado será comunicada al deudor afectado, que podrá formular alegaciones en el plazo de 10 días contados a partir del siguiente al de recepción de la comunicación. A estos efectos será suficiente para entender realizada dicha comunicación la acreditación por parte de la Administración Tributaria de haber realizado un intento de notificación de la misma que contenga el texto íntegro de su contenido en el domicilio fiscal del interesado.

Las alegaciones habrán de referirse exclusivamente a la existencia de errores materiales, de hecho o aritméticos en relación con los requisitos señalados en el apartado 1.

Como consecuencia del trámite de alegaciones, la Administración podrá acordar la rectificación del listado cuando se acredite fehacientemente que no concurren los requisitos legales determinados en el apartado 1.

Dicha rectificación también podrá ser acordada de oficio.

Practicadas las rectificaciones oportunas, se dictará el acuerdo de publicación.

La notificación del acuerdo se entenderá producida con su publicación y la del listado.

Mediante Orden Ministerial se establecerán la fecha de publicación, que deberá producirse en todo caso durante el primer semestre de cada año, y los correspondientes ficheros y registros.

La publicación se efectuará en todo caso por medios electrónicos, debiendo adoptarse las medidas necesarias para impedir la indexación de su contenido a través de motores de búsqueda en Internet y los listados dejarán de ser accesibles una vez transcurridos tres meses desde la fecha de publicación.

El tratamiento de datos necesarios para la publicación se sujetará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter general, y en su Reglamento aprobado por Real Decreto 1720/2007, de 21 de diciembre.

5. En el ámbito de competencias del Estado, será competente para dictar los acuerdos de publicación regulados en este artículo el Director General de la Agencia Estatal de Administración Tributaria.

6. En la publicación del listado se especificará que la situación en el mismo reflejada es la existente a la fecha de referencia señalada en el apartado 4, sin que la publicación del listado resulte afectada por las actuaciones realizadas por el deudor con posterioridad a dicha fecha de referencia, en orden al pago de las deudas y sanciones incluidas en el mismo.

Lo dispuesto en este artículo no afectará en modo alguno al régimen de impugnación establecido en esta Ley en relación con las actuaciones y procedimientos de los que se deriven las deudas y sanciones tributarias ni tampoco a las actuaciones y procedimientos de aplicación de los tributos iniciados o que se pudieran iniciar con posterioridad en relación con las mismas.

Las actuaciones desarrolladas en el procedimiento establecido en este artículo en orden a la publicación de la información en el mismo regulada no constituyen causa de interrupción a los efectos previstos en el artículo 68 de esta Ley.

7. El acuerdo de publicación del listado pondrá fin a la vía administrativa.

[. . .]

§ 58

Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 264, de 4 de noviembre de 2003
Última modificación: 4 de julio de 2018
Referencia: BOE-A-2003-20254

[. . .]

TÍTULO V

Gestión patrimonial

[. . .]

CAPÍTULO V

Enajenación y gravamen

[. . .]

Sección 2.ª Enajenación de inmuebles

[. . .]

Artículo 138. *Procedimiento de enajenación.*

1. El expediente de enajenación de bienes inmuebles y derechos sobre los mismos pertenecientes al patrimonio de la Administración General del Estado será instruido por la Dirección General del Patrimonio del Estado que lo iniciará de oficio, por iniciativa propia o a solicitud de parte interesada en la adquisición, siempre que considere, justificándolo debidamente en el expediente, que el bien o derecho no es necesario para el uso general o el servicio público ni resulta conveniente su explotación. El acuerdo de incoación del procedimiento llevará implícita la declaración de alienabilidad de los bienes a que se refiera.

Podrá acordarse la enajenación de los inmuebles por lotes y, en los supuestos de enajenación directa, admitirse la entrega de otros inmuebles o derechos sobre los mismos en pago de parte del precio de venta, valorados de conformidad con el artículo 114 de esta ley.

2. El tipo de la subasta o el precio de la enajenación directa se fijarán por el órgano competente para la enajenación de acuerdo con la tasación aprobada. De igual forma, los pliegos que han de regir el concurso determinarán los criterios que hayan de tenerse en cuenta en la adjudicación, atendiendo a las directrices que resulten de las políticas públicas de cuya aplicación se trate. En todo caso, los pliegos harán referencia a la situación física, jurídica y registral de la finca.

3. La convocatoria del procedimiento de enajenación se publicará gratuitamente en el "Boletín Oficial del Estado" y en el de la provincia en que radique el bien y se remitirá al ayuntamiento del correspondiente término municipal para su exhibición en el tablón de anuncios, sin perjuicio de la posibilidad de utilizar, además, otros medios de publicidad, atendida la naturaleza y características del bien.

La Dirección General del Patrimonio del Estado podrá establecer otros mecanismos complementarios tendentes a difundir información sobre los bienes inmuebles en proceso de venta, incluida la creación, con sujeción a las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, de ficheros con los datos de las personas que voluntaria y expresamente soliciten les sea remitida información sobre dichos bienes.

4. La suspensión del procedimiento, una vez efectuado el anuncio, sólo podrá efectuarse por Orden del Ministro de Hacienda, cuando se trate de bienes de la Administración General del Estado, o por acuerdo de los presidentes o directores de los organismos públicos, cuando se trate de bienes propios de éstos, con fundamento en documentos fehacientes o hechos acreditados que prueben la improcedencia de la venta.

5. El Ministro de Hacienda, a propuesta de la Dirección General del Patrimonio del Estado, o los presidentes o directores de los organismos públicos acordarán, previo informe de la Abogacía del Estado o del órgano al que corresponda el asesoramiento jurídico de las entidades públicas, la enajenación o su improcedencia, si considerasen perjudicial para el interés público la adjudicación en las condiciones propuestas o si, por razones sobrevenidas, considerasen necesario el bien para el cumplimiento de fines públicos, sin que la instrucción del expediente, la celebración de la subasta o la valoración de las proposiciones presentadas generen derecho alguno para quienes optaron a su compra.

[. . .]

§ 59

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

Jefatura del Estado
«BOE» núm. 274, de 15 de noviembre de 2002
Última modificación: 22 de septiembre de 2015
Referencia: BOE-A-2002-22188

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

EXPOSICIÓN DE MOTIVOS

La importancia que tienen los derechos de los pacientes como eje básico de las relaciones clínico-asistenciales se pone de manifiesto al constatar el interés que han demostrado por los mismos casi todas las organizaciones internacionales con competencia en la materia. Ya desde el fin de la Segunda Guerra Mundial, organizaciones como Naciones Unidas, UNESCO o la Organización Mundial de la Salud, o, más recientemente, la Unión Europea o el Consejo de Europa, entre muchas otras, han impulsado declaraciones o, en algún caso, han promulgado normas jurídicas sobre aspectos genéricos o específicos relacionados con esta cuestión. En este sentido, es necesario mencionar la trascendencia de la Declaración universal de derechos humanos, del año 1948, que ha sido el punto de referencia obligado para todos los textos constitucionales promulgados posteriormente o, en el ámbito más estrictamente sanitario, la Declaración sobre la promoción de los derechos de los pacientes en Europa, promovida el año 1994 por la Oficina Regional para Europa de la Organización Mundial de la Salud, aparte de múltiples declaraciones internacionales de mayor o menor alcance e influencia que se han referido a dichas cuestiones.

Últimamente, cabe subrayar la relevancia especial del Convenio del Consejo de Europa para la protección de los derechos humanos y la dignidad del ser humano respecto de las aplicaciones de la biología y la medicina (Convenio sobre los derechos del hombre y la biomedicina), suscrito el día 4 de abril de 1997, el cual ha entrado en vigor en el Reino de España el 1 de enero de 2000. Dicho Convenio es una iniciativa capital: en efecto, a diferencia de las distintas declaraciones internacionales que lo han precedido, es el primer instrumento internacional con carácter jurídico vinculante para los países que lo suscriben. Su especial valía reside en el hecho de que establece un marco común para la protección de

los derechos humanos y la dignidad humana en la aplicación de la biología y la medicina. El Convenio trata explícitamente, con detenimiento y extensión, sobre la necesidad de reconocer los derechos de los pacientes, entre los cuales resaltan el derecho a la información, el consentimiento informado y la intimidad de la información relativa a la salud de las personas, persiguiendo el alcance de una armonización de las legislaciones de los diversos países en estas materias; en este sentido, es absolutamente conveniente tener en cuenta el Convenio en el momento de abordar el reto de regular cuestiones tan importantes.

Es preciso decir, sin embargo, que la regulación del derecho a la protección de la salud, recogido por el artículo 43 de la Constitución de 1978, desde el punto de vista de las cuestiones más estrechamente vinculadas a la condición de sujetos de derechos de las personas usuarias de los servicios sanitarios, es decir, la plasmación de los derechos relativos a la información clínica y la autonomía individual de los pacientes en lo relativo a su salud, ha sido objeto de una regulación básica en el ámbito del Estado, a través de la Ley 14/1986, de 25 de abril, General de Sanidad.

De otra parte, esta Ley, a pesar de que fija básicamente su atención en el establecimiento y ordenación del sistema sanitario desde un punto de vista organizativo, dedica a esta cuestión diversas previsiones, entre las que destaca la voluntad de humanización de los servicios sanitarios. Así mantiene el máximo respeto a la dignidad de la persona y a la libertad individual, de un lado, y, del otro, declara que la organización sanitaria debe permitir garantizar la salud como derecho inalienable de la población mediante la estructura del Sistema Nacional de Salud, que debe asegurarse en condiciones de escrupuloso respeto a la intimidad personal y a la libertad individual del usuario, garantizando la confidencialidad de la información relacionada con los servicios sanitarios que se prestan y sin ningún tipo de discriminación.

A partir de dichas premisas, la presente Ley completa las previsiones que la Ley General de Sanidad enunció como principios generales. En este sentido, refuerza y da un trato especial al derecho a la autonomía del paciente. En particular, merece mención especial la regulación sobre instrucciones previas que contempla, de acuerdo con el criterio establecido en el Convenio de Oviedo, los deseos del paciente expresados con anterioridad dentro del ámbito del consentimiento informado. Asimismo, la Ley trata con profundidad todo lo referente a la documentación clínica generada en los centros asistenciales, subrayando especialmente la consideración y la concreción de los derechos de los usuarios en este aspecto.

En septiembre de 1997, en desarrollo de un convenio de colaboración entre el Consejo General del Poder Judicial y el Ministerio de Sanidad y Consumo, tuvo lugar un seminario conjunto sobre información y documentación clínica, en el que se debatieron los principales aspectos normativos y judiciales en la materia. Al mismo tiempo, se constituyó un grupo de expertos a quienes se encargó la elaboración de unas directrices para el desarrollo futuro de este tema. Este grupo suscribió un dictamen el 26 de noviembre de 1997, que ha sido tenido en cuenta en la elaboración de los principios fundamentales de esta Ley.

La atención que a estas materias otorgó en su día la Ley General de Sanidad supuso un notable avance como reflejan, entre otros, sus artículos 9, 10 y 61. Sin embargo, el derecho a la información, como derecho del ciudadano cuando demanda la atención sanitaria, ha sido objeto en los últimos años de diversas matizaciones y ampliaciones por Leyes y disposiciones de distinto tipo y rango, que ponen de manifiesto la necesidad de una reforma y actualización de la normativa contenida en la Ley General de Sanidad. Así, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, califica a los datos relativos a la salud de los ciudadanos como datos especialmente protegidos, estableciendo un régimen singularmente riguroso para su obtención, custodia y eventual cesión.

Esta defensa de la confidencialidad había sido ya defendida por la Directiva comunitaria 95/46, de 24 de octubre, en la que, además de reafirmarse la defensa de los derechos y libertades de los ciudadanos europeos, en especial de su intimidad relativa a la información relacionada con su salud, se apunta la presencia de otros intereses generales como los estudios epidemiológicos, las situaciones de riesgo grave para la salud de la colectividad, la investigación y los ensayos clínicos que, cuando estén incluidos en normas de rango de Ley, pueden justificar una excepción motivada a los derechos del paciente. Se manifiesta así una

concepción comunitaria del derecho a la salud, en la que, junto al interés singular de cada individuo, como destinatario por excelencia de la información relativa a la salud, aparecen también otros agentes y bienes jurídicos referidos a la salud pública, que deben ser considerados, con la relevancia necesaria, en una sociedad democrática avanzada. En esta línea, el Consejo de Europa, en su Recomendación de 13 de febrero de 1997, relativa a la protección de los datos médicos, después de afirmar que deben recogerse y procesarse con el consentimiento del afectado, indica que la información puede restringirse si así lo dispone una Ley y constituye una medida necesaria por razones de interés general.

Todas estas circunstancias aconsejan una adaptación de la Ley General de Sanidad con el objetivo de aclarar la situación jurídica y los derechos y obligaciones de los profesionales sanitarios, de los ciudadanos y de las instituciones sanitarias. Se trata de ofrecer en el terreno de la información y la documentación clínicas las mismas garantías a todos los ciudadanos del Estado, fortaleciendo con ello el derecho a la protección de la salud que reconoce la Constitución.

CAPÍTULO I

Principios generales

Artículo 1. *Ámbito de aplicación.*

La presente Ley tiene por objeto la regulación de los derechos y obligaciones de los pacientes, usuarios y profesionales, así como de los centros y servicios sanitarios, públicos y privados, en materia de autonomía del paciente y de información y documentación clínica.

Artículo 2. *Principios básicos.*

1. La dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica.

2. Toda actuación en el ámbito de la sanidad requiere, con carácter general, el previo consentimiento de los pacientes o usuarios. El consentimiento, que debe obtenerse después de que el paciente reciba una información adecuada, se hará por escrito en los supuestos previstos en la Ley.

3. El paciente o usuario tiene derecho a decidir libremente, después de recibir la información adecuada, entre las opciones clínicas disponibles.

4. Todo paciente o usuario tiene derecho a negarse al tratamiento, excepto en los casos determinados en la Ley. Su negativa al tratamiento constará por escrito.

5. Los pacientes o usuarios tienen el deber de facilitar los datos sobre su estado físico o sobre su salud de manera leal y verdadera, así como el de colaborar en su obtención, especialmente cuando sean necesarios por razones de interés público o con motivo de la asistencia sanitaria.

6. Todo profesional que interviene en la actividad asistencial está obligado no sólo a la correcta prestación de sus técnicas, sino al cumplimiento de los deberes de información y de documentación clínica, y al respeto de las decisiones adoptadas libre y voluntariamente por el paciente.

7. La persona que elabore o tenga acceso a la información y la documentación clínica está obligada a guardar la reserva debida.

Artículo 3. *Las definiciones legales.*

A efectos de esta Ley se entiende por:

Centro sanitario: el conjunto organizado de profesionales, instalaciones y medios técnicos que realiza actividades y presta servicios para cuidar la salud de los pacientes y usuarios.

Certificado médico: la declaración escrita de un médico que da fe del estado de salud de una persona en un determinado momento.

Consentimiento informado: la conformidad libre, voluntaria y consciente de un paciente, manifestada en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar una actuación que afecta a su salud.

Documentación clínica: el soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial.

Historia clínica: el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial.

Información clínica: todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla.

Informe de alta médica: el documento emitido por el médico responsable en un centro sanitario al finalizar cada proceso asistencial de un paciente, que especifica los datos de éste, un resumen de su historial clínico, la actividad asistencial prestada, el diagnóstico y las recomendaciones terapéuticas.

Intervención en el ámbito de la sanidad: toda actuación realizada con fines preventivos, diagnósticos, terapéuticos, rehabilitadores o de investigación.

Libre elección: la facultad del paciente o usuario de optar, libre y voluntariamente, entre dos o más alternativas asistenciales, entre varios facultativos o entre centros asistenciales, en los términos y condiciones que establezcan los servicios de salud competentes, en cada caso.

Médico responsable: el profesional que tiene a su cargo coordinar la información y la asistencia sanitaria del paciente o del usuario, con el carácter de interlocutor principal del mismo en todo lo referente a su atención e información durante el proceso asistencial, sin perjuicio de las obligaciones de otros profesionales que participan en las actuaciones asistenciales.

Paciente: la persona que requiere asistencia sanitaria y está sometida a cuidados profesionales para el mantenimiento o recuperación de su salud.

Servicio sanitario: la unidad asistencial con organización propia, dotada de los recursos técnicos y del personal cualificado para llevar a cabo actividades sanitarias.

Usuario: la persona que utiliza los servicios sanitarios de educación y promoción de la salud, de prevención de enfermedades y de información sanitaria.

CAPÍTULO II

El derecho de información sanitaria

Artículo 4. *Derecho a la información asistencial.*

1. Los pacientes tienen derecho a conocer, con motivo de cualquier actuación en el ámbito de su salud, toda la información disponible sobre la misma, salvando los supuestos exceptuados por la Ley. Además, toda persona tiene derecho a que se respete su voluntad de no ser informada. La información, que como regla general se proporcionará verbalmente dejando constancia en la historia clínica, comprende, como mínimo, la finalidad y la naturaleza de cada intervención, sus riesgos y sus consecuencias.

2. La información clínica forma parte de todas las actuaciones asistenciales, será verdadera, se comunicará al paciente de forma comprensible y adecuada a sus necesidades y le ayudará a tomar decisiones de acuerdo con su propia y libre voluntad.

3. El médico responsable del paciente le garantiza el cumplimiento de su derecho a la información. Los profesionales que le atiendan durante el proceso asistencial o le apliquen una técnica o un procedimiento concreto también serán responsables de informarle.

Artículo 5. *Titular del derecho a la información asistencial.*

1. El titular del derecho a la información es el paciente. También serán informadas las personas vinculadas a él, por razones familiares o de hecho, en la medida que el paciente lo permita de manera expresa o tácita.

2. El paciente será informado, incluso en caso de incapacidad, de modo adecuado a sus posibilidades de comprensión, cumpliendo con el deber de informar también a su representante legal.

3. Cuando el paciente, según el criterio del médico que le asiste, carezca de capacidad para entender la información a causa de su estado físico o psíquico, la información se pondrá en conocimiento de las personas vinculadas a él por razones familiares o de hecho.

4. El derecho a la información sanitaria de los pacientes puede limitarse por la existencia acreditada de un estado de necesidad terapéutica. Se entenderá por necesidad terapéutica la facultad del médico para actuar profesionalmente sin informar antes al paciente, cuando por razones objetivas el conocimiento de su propia situación pueda perjudicar su salud de manera grave.

Llegado este caso, el médico dejará constancia razonada de las circunstancias en la historia clínica y comunicará su decisión a las personas vinculadas al paciente por razones familiares o de hecho.

Artículo 6. *Derecho a la información epidemiológica.*

Los ciudadanos tienen derecho a conocer los problemas sanitarios de la colectividad cuando impliquen un riesgo para la salud pública o para su salud individual, y el derecho a que esta información se difunda en términos verdaderos, comprensibles y adecuados para la protección de la salud, de acuerdo con lo establecido por la Ley.

CAPÍTULO III

Derecho a la intimidad

Artículo 7. *El derecho a la intimidad.*

1. Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.

2. Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes.

CAPÍTULO IV

El respeto de la autonomía del paciente

Artículo 8. *Consentimiento informado.*

1. Toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado, una vez que, recibida la información prevista en el artículo 4, haya valorado las opciones propias del caso.

2. El consentimiento será verbal por regla general.

Sin embargo, se prestará por escrito en los casos siguientes: intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente.

3. El consentimiento escrito del paciente será necesario para cada una de las actuaciones especificadas en el punto anterior de este artículo, dejando a salvo la posibilidad de incorporar anejos y otros datos de carácter general, y tendrá información suficiente sobre el procedimiento de aplicación y sobre sus riesgos.

4. Todo paciente o usuario tiene derecho a ser advertido sobre la posibilidad de utilizar los procedimientos de pronóstico, diagnóstico y terapéuticos que se le apliquen en un proyecto docente o de investigación, que en ningún caso podrá comportar riesgo adicional para su salud.

5. El paciente puede revocar libremente por escrito su consentimiento en cualquier momento.

Artículo 9. *Límites del consentimiento informado y consentimiento por representación.*

1. La renuncia del paciente a recibir información está limitada por el interés de la salud del propio paciente, de terceros, de la colectividad y por las exigencias terapéuticas del caso. Cuando el paciente manifieste expresamente su deseo de no ser informado, se respetará su voluntad haciendo constar su renuncia documentalmente, sin perjuicio de la obtención de su consentimiento previo para la intervención.

2. Los facultativos podrán llevar a cabo las intervenciones clínicas indispensables en favor de la salud del paciente, sin necesidad de contar con su consentimiento, en los siguientes casos:

a) Cuando existe riesgo para la salud pública a causa de razones sanitarias establecidas por la Ley. En todo caso, una vez adoptadas las medidas pertinentes, de conformidad con lo establecido en la Ley Orgánica 3/1986, se comunicarán a la autoridad judicial en el plazo máximo de 24 horas siempre que dispongan el internamiento obligatorio de personas.

b) Cuando existe riesgo inmediato grave para la integridad física o psíquica del enfermo y no es posible conseguir su autorización, consultando, cuando las circunstancias lo permitan, a sus familiares o a las personas vinculadas de hecho a él.

3. Se otorgará el consentimiento por representación en los siguientes supuestos:

a) Cuando el paciente no sea capaz de tomar decisiones, a criterio del médico responsable de la asistencia, o su estado físico o psíquico no le permita hacerse cargo de su situación. Si el paciente carece de representante legal, el consentimiento lo prestarán las personas vinculadas a él por razones familiares o de hecho.

b) Cuando el paciente tenga la capacidad modificada judicialmente y así conste en la sentencia.

c) Cuando el paciente menor de edad no sea capaz intelectual ni emocionalmente de comprender el alcance de la intervención. En este caso, el consentimiento lo dará el representante legal del menor, después de haber escuchado su opinión, conforme a lo dispuesto en el artículo 9 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

4. Cuando se trate de menores emancipados o mayores de 16 años que no se encuentren en los supuestos b) y c) del apartado anterior, no cabe prestar el consentimiento por representación.

No obstante lo dispuesto en el párrafo anterior, cuando se trate de una actuación de grave riesgo para la vida o salud del menor, según el criterio del facultativo, el consentimiento lo prestará el representante legal del menor, una vez oída y tenida en cuenta la opinión del mismo.

5. La práctica de ensayos clínicos y la práctica de técnicas de reproducción humana asistida se rigen por lo establecido con carácter general sobre la mayoría de edad y por las disposiciones especiales de aplicación.

Para la interrupción voluntaria del embarazo de menores de edad o personas con capacidad modificada judicialmente será preciso, además de su manifestación de voluntad, el consentimiento expreso de sus representantes legales. En este caso, los conflictos que surjan en cuanto a la prestación del consentimiento por parte de los representantes legales, se resolverán de conformidad con lo dispuesto en el Código Civil.

6. En los casos en los que el consentimiento haya de otorgarlo el representante legal o las personas vinculadas por razones familiares o de hecho en cualquiera de los supuestos descritos en los apartados 3 a 5, la decisión deberá adoptarse atendiendo siempre al mayor beneficio para la vida o salud del paciente. Aquellas decisiones que sean contrarias a dichos intereses deberán ponerse en conocimiento de la autoridad judicial, directamente o a través del Ministerio Fiscal, para que adopte la resolución correspondiente, salvo que, por razones de urgencia, no fuera posible recabar la autorización judicial, en cuyo caso los profesionales sanitarios adoptarán las medidas necesarias en salvaguarda de la vida o salud del paciente, amparados por las causas de justificación de cumplimiento de un deber y de estado de necesidad.

7. La prestación del consentimiento por representación será adecuada a las circunstancias y proporcionada a las necesidades que haya que atender, siempre en favor del paciente y con respeto a su dignidad personal. El paciente participará en la medida de lo posible en la toma de decisiones a lo largo del proceso sanitario. Si el paciente es una persona con discapacidad, se le ofrecerán las medidas de apoyo pertinentes, incluida la información en formatos adecuados, siguiendo las reglas marcadas por el principio del diseño para todos de manera que resulten accesibles y comprensibles a las personas con discapacidad, para favorecer que pueda prestar por sí su consentimiento.

Artículo 10. *Condiciones de la información y consentimiento por escrito.*

1. El facultativo proporcionará al paciente, antes de recabar su consentimiento escrito, la información básica siguiente:

a) Las consecuencias relevantes o de importancia que la intervención origina con seguridad.
b) Los riesgos relacionados con las circunstancias personales o profesionales del paciente.
c) Los riesgos probables en condiciones normales, conforme a la experiencia y al estado de la ciencia o directamente relacionados con el tipo de intervención.
d) Las contraindicaciones.

2. El médico responsable deberá ponderar en cada caso que cuanto más dudoso sea el resultado de una intervención más necesario resulta el previo consentimiento por escrito del paciente.

Artículo 11. *Instrucciones previas.*

1. Por el documento de instrucciones previas, una persona mayor de edad, capaz y libre, manifiesta anticipadamente su voluntad, con objeto de que ésta se cumpla en el momento en que llegue a situaciones en cuyas circunstancias no sea capaz de expresarlos personalmente, sobre los cuidados y el tratamiento de su salud o, una vez llegado el fallecimiento, sobre el destino de su cuerpo o de los órganos del mismo. El otorgante del documento puede designar, además, un representante para que, llegado el caso, sirva como interlocutor suyo con el médico o el equipo sanitario para procurar el cumplimiento de las instrucciones previas.
2. Cada servicio de salud regulará el procedimiento adecuado para que, llegado el caso, se garantice el cumplimiento de las instrucciones previas de cada persona, que deberán constar siempre por escrito.
3. No serán aplicadas las instrucciones previas contrarias al ordenamiento jurídico, a la «lex artis», ni las que no se correspondan con el supuesto de hecho que el interesado haya previsto en el momento de manifestarlas. En la historia clínica del paciente quedará constancia razonada de las anotaciones relacionadas con estas previsiones.
4. Las instrucciones previas podrán revocarse libremente en cualquier momento dejando constancia por escrito.
5. Con el fin de asegurar la eficacia en todo el territorio nacional de las instrucciones previas manifestadas por los pacientes y formalizadas de acuerdo con lo dispuesto en la legislación de las respectivas Comunidades Autónomas, se creará en el Ministerio de Sanidad y Consumo el Registro nacional de instrucciones previas que se regirá por las normas que reglamentariamente se determinen, previo acuerdo del Consejo Interterritorial del Sistema Nacional de Salud.

Artículo 12. *Información en el Sistema Nacional de Salud.*

1. Además de los derechos reconocidos en los artículos anteriores, los pacientes y los usuarios del Sistema Nacional de Salud tendrán derecho a recibir información sobre los servicios y unidades asistenciales disponibles, su calidad y los requisitos de acceso a ellos.
2. Los servicios de salud dispondrán en los centros y servicios sanitarios de una guía o carta de los servicios en la que se especifiquen los derechos y obligaciones de los usuarios,

las prestaciones disponibles, las características asistenciales del centro o del servicio, y sus dotaciones de personal, instalaciones y medios técnicos.

Se facilitará a todos los usuarios información sobre las guías de participación y sobre sugerencias y reclamaciones.

3. Cada servicio de salud regulará los procedimientos y los sistemas para garantizar el efectivo cumplimiento de las previsiones de este artículo.

Artículo 13. *Derecho a la información para la elección de médico y de centro.*

Los usuarios y pacientes del Sistema Nacional de Salud, tanto en la atención primaria como en la especializada, tendrán derecho a la información previa correspondiente para elegir médico, e igualmente centro, con arreglo a los términos y condiciones que establezcan los servicios de salud competentes.

CAPÍTULO V

La historia clínica

Artículo 14. *Definición y archivo de la historia clínica.*

1. La historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro.

2. Cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información.

3. Las Administraciones sanitarias establecerán los mecanismos que garanticen la autenticidad del contenido de la historia clínica y de los cambios operados en ella, así como la posibilidad de su reproducción futura.

4. Las Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental.

Artículo 15. *Contenido de la historia clínica de cada paciente.*

1. La historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. Todo paciente o usuario tiene derecho a que quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada.

2. La historia clínica tendrá como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud.

El contenido mínimo de la historia clínica será el siguiente:

a) La documentación relativa a la hoja clínicoestadística.
b) La autorización de ingreso.
c) El informe de urgencia.
d) La anamnesis y la exploración física.
e) La evolución.
f) Las órdenes médicas.
g) La hoja de interconsulta.
h) Los informes de exploraciones complementarias.
i) El consentimiento informado.
j) El informe de anestesia.
k) El informe de quirófano o de registro del parto.
l) El informe de anatomía patológica.

m) La evolución y planificación de cuidados de enfermería.
n) La aplicación terapéutica de enfermería.
ñ) El gráfico de constantes.
o) El informe clínico de alta.

Los párrafos b), c), i), j), k), l), ñ) y o) sólo serán exigibles en la cumplimentación de la historia clínica cuando se trate de procesos de hospitalización o así se disponga.

3. Cuando se trate del nacimiento, la historia clínica incorporará, además de la información a la que hace referencia este apartado, los resultados de las pruebas biométricas, médicas o analíticas que resulten, en su caso, necesarias para determinar el vínculo de filiación con la madre, en los términos que se establezcan reglamentariamente.

4. La historia clínica se llevará con criterios de unidad y de integración, en cada institución asistencial como mínimo, para facilitar el mejor y más oportuno conocimiento por los facultativos de los datos de un determinado paciente en cada proceso asistencial.

Artículo 16. *Usos de la historia clínica.*

1. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.

2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.

4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.

5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.

6. El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.

7. Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso.

Artículo 17. *La conservación de la documentación clínica.*

1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no

necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.

No obstante, los datos de la historia clínica relacionados con el nacimiento del paciente, incluidos los resultados de las pruebas biométricas, médicas o analíticas que en su caso resulten necesarias para determinar el vínculo de filiación con la madre, no se destruirán, trasladándose una vez conocido el fallecimiento del paciente, a los archivos definitivos de la Administración correspondiente, donde se conservarán con las debidas medidas de seguridad a los efectos de la legislación de protección de datos.

2. La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas.

Sin perjuicio del derecho al que se refiere el artículo siguiente, los datos de la historia clínica relacionados con las pruebas biométricas, médicas o analíticas que resulten necesarias para determinar el vínculo de filiación con la madre del recién nacido, sólo podrán ser comunicados a petición judicial, dentro del correspondiente proceso penal o en caso de reclamación o impugnación judicial de la filiación materna.

3. Los profesionales sanitarios tienen el deber de cooperar en la creación y el mantenimiento de una documentación clínica ordenada y secuencial del proceso asistencial de los pacientes.

4. La gestión de la historia clínica por los centros con pacientes hospitalizados, o por los que atiendan a un número suficiente de pacientes bajo cualquier otra modalidad asistencial, según el criterio de los servicios de salud, se realizará a través de la unidad de admisión y documentación clínica, encargada de integrar en un solo archivo las historias clínicas. La custodia de dichas historias clínicas estará bajo la responsabilidad de la dirección del centro sanitario.

5. Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen.

6. Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

Artículo 18. *Derechos de acceso a la historia clínica.*

1. El paciente tiene el derecho de acceso, con las reservas señaladas en el apartado 3 de este artículo, a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella. Los centros sanitarios regularán el procedimiento que garantice la observancia de estos derechos.

2. El derecho de acceso del paciente a la historia clínica puede ejercerse también por representación debidamente acreditada.

3. El derecho al acceso del paciente a la documentación de la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas.

4. Los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros.

Artículo 19. *Derechos relacionados con la custodia de la historia clínica.*

El paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido por el artículo 16 de la presente Ley.

CAPÍTULO VI

Informe de alta y otra documentación clínica

Artículo 20. *Informe de alta.*

Todo paciente, familiar o persona vinculada a él, en su caso, tendrá el derecho a recibir del centro o servicio sanitario, una vez finalizado el proceso asistencial, un informe de alta con los contenidos mínimos que determina el artículo 3. Las características, requisitos y condiciones de los informes de alta se determinarán reglamentariamente por las Administraciones sanitarias autonómicas.

Artículo 21. *El alta del paciente.*

1. En caso de no aceptar el tratamiento prescrito, se propondrá al paciente o usuario la firma del alta voluntaria. Si no la firmara, la dirección del centro sanitario, a propuesta del médico responsable, podrá disponer el alta forzosa en las condiciones reguladas por la Ley.

El hecho de no aceptar el tratamiento prescrito no dará lugar al alta forzosa cuando existan tratamientos alternativos, aunque tengan carácter paliativo, siempre que los preste el centro sanitario y el paciente acepte recibirlos. Estas circunstancias quedarán debidamente documentadas.

2. En el caso de que el paciente no acepte el alta, la dirección del centro, previa comprobación del informe clínico correspondiente, oirá al paciente y, si persiste en su negativa, lo pondrá en conocimiento del juez para que confirme o revoque la decisión.

Artículo 22. *Emisión de certificados médicos.*

Todo paciente o usuario tiene derecho a que se le faciliten los certificados acreditativos de su estado de salud. Éstos serán gratuitos cuando así lo establezca una disposición legal o reglamentaria.

Artículo 23. *Obligaciones profesionales de información técnica, estadística y administrativa.*

Los profesionales sanitarios, además de las obligaciones señaladas en materia de información clínica, tienen el deber de cumplimentar los protocolos, registros, informes, estadísticas y demás documentación asistencial o administrativa, que guarden relación con los procesos clínicos en los que intervienen, y los que requieran los centros o servicios de salud competentes y las autoridades sanitarias, comprendidos los relacionados con la investigación médica y la información epidemiológica.

Disposición adicional primera. *Carácter de legislación básica.*

Esta Ley tiene la condición de básica, de conformidad con lo establecido en el artículo 149.1.1.ª y 16.ª de la Constitución.

El Estado y las Comunidades Autónomas adoptarán, en el ámbito de sus respectivas competencias, las medidas necesarias para la efectividad de esta Ley.

Disposición adicional segunda. *Aplicación supletoria.*

Las normas de esta Ley relativas a la información asistencial, la información para el ejercicio de la libertad de elección de médico y de centro, el consentimiento informado del paciente y la documentación clínica, serán de aplicación supletoria en los proyectos de investigación médica, en los procesos de extracción y trasplante de órganos, en los de

aplicación de técnicas de reproducción humana asistida y en los que carezcan de regulación especial.

Disposición adicional tercera. *Coordinación de las historias clínicas.*

El Ministerio de Sanidad y Consumo, en coordinación y con la colaboración de las Comunidades Autónomas competentes en la materia, promoverá, con la participación de todos los interesados, la implantación de un sistema de compatibilidad que, atendida la evolución y disponibilidad de los recursos técnicos, y la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición.

Disposición adicional cuarta. *Necesidades asociadas a la discapacidad.*

El Estado y las Comunidades Autónomas, dentro del ámbito de sus respectivas competencias, dictarán las disposiciones precisas para garantizar a los pacientes o usuarios con necesidades especiales, asociadas a la discapacidad, los derechos en materia de autonomía, información y documentación clínica regulados en esta Ley.

Disposición adicional quinta. *Información y documentación sobre medicamentos y productos sanitarios.*

La información, la documentación y la publicidad relativas a los medicamentos y productos sanitarios, así como el régimen de las recetas y de las órdenes de prescripción correspondientes, se regularán por su normativa específica, sin perjuicio de la aplicación de las reglas establecidas en esta Ley en cuanto a la prescripción y uso de medicamentos o productos sanitarios durante los procesos asistenciales.

Disposición adicional sexta. *Régimen sancionador.*

Las infracciones de lo dispuesto por la presente Ley quedan sometidas al régimen sancionador previsto en el capítulo VI del Título I de la Ley 14/1986, General de Sanidad, sin perjuicio de la responsabilidad civil o penal y de la responsabilidad profesional o estatutaria procedentes en derecho.

Disposición transitoria única. *Informe de alta.*

El informe de alta se regirá por lo dispuesto en la Orden del Ministerio de Sanidad, de 6 de septiembre de 1984, mientras no se desarrolle legalmente lo dispuesto en el artículo 20 de esta Ley.

Disposición derogatoria única. *Derogación general y de preceptos concretos.*

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en la presente Ley y, concretamente, los apartados 5, 6, 8, 9 y 11 del artículo 10, el apartado 4 del artículo 11 y el artículo 61 de la Ley 14/1986, General de Sanidad.

Disposición final única. *Entrada en vigor.*

La presente Ley entrará en vigor en el plazo de seis meses a partir del día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 60

Ley Orgánica 1/2002, de 22 de marzo, reguladora del Derecho de Asociación. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 73, de 26 de marzo de 2002
Última modificación: 23 de septiembre de 2011
Referencia: BOE-A-2002-5852

[. . .]

CAPÍTULO III

Funcionamiento de las asociaciones

[. . .]

Artículo 14. *Obligaciones documentales y contables.*

1. Las asociaciones han de disponer de una relación actualizada de sus asociados, llevar una contabilidad que permita obtener la imagen fiel del patrimonio, del resultado y de la situación financiera de la entidad, así como las actividades realizadas, efectuar un inventario de sus bienes y recoger en un libro las actas de las reuniones de sus órganos de gobierno y representación. Deberán llevar su contabilidad conforme a las normas específicas que les resulten de aplicación.

2. Los asociados podrán acceder a toda la documentación- que se relaciona en el apartado anterior, a través de los órganos de representación, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

3. Las cuentas de la asociación se aprobarán anualmente por la Asamblea General.

[. . .]

CAPÍTULO V

Registros de Asociaciones

[. . .]

Artículo 29. *Publicidad.*

1. Los Registros de Asociaciones son públicos.

2. La publicidad se hará efectiva mediante certificación del contenido de los asientos, por nota simple informativa o por copia de los asientos y de los documentos depositados en los Registros o por medios informáticos o telemáticos que se ajustará a los requisitos establecidos en la normativa vigente en materia de protección de datos de carácter personal.

[. . .]

§ 61

Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 11, de 13 de enero de 2000
Última modificación: 28 de diciembre de 2012
Referencia: BOE-A-2000-641

[. . .]

TÍTULO VII

De la ejecución de las medidas

[. . .]

CAPÍTULO II

Reglas para la ejecución de las medidas

[. . .]

Artículo 48. *Expediente personal de la persona sometida a la ejecución de una medida.*

1. La entidad pública abrirá un expediente personal único a cada menor respecto del cual tenga encomendada la ejecución de una medida, en el que se recogerán los informes relativos a aquél, las resoluciones judiciales que le afecten y el resto de la documentación generada durante la ejecución.

2. Dicho expediente tendrá carácter reservado y solamente tendrán acceso al mismo el Defensor del Pueblo o institución análoga de la correspondiente Comunidad Autónoma, los Jueces de Menores competentes, el Ministerio Fiscal y las personas que intervengan en la ejecución y estén autorizadas por la entidad pública de acuerdo con sus normas de organización. El menor, su letrado y, en su caso, su representante legal, también tendrán acceso al expediente.

3. La recogida, cesión y tratamiento automatizado de datos de carácter personal de las personas a las que se aplique la presente Ley, sólo podrá realizarse en ficheros informáticos de titularidad pública dependientes de las entidades públicas de protección de menores, Administraciones y Juzgados de Menores competentes o del Ministerio Fiscal, y se regirá por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Cáracter Personal, y sus normas de desarrollo.

[. . .]

Disposición adicional tercera. *Registro de sentencias firmes dictadas en aplicación de lo dispuesto en la presente Ley.*

En el Ministerio de Justicia se llevará un Registro de sentencias firmes dictadas en aplicación de lo dispuesto en la presente Ley, cuyos datos sólo podrán ser utilizados por los Jueces de Menores y por el Ministerio Fiscal a efectos de lo establecido en los artículos 6, 30 y 47 de esta Ley, teniendo en cuenta lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y sus disposiciones complementarias.

[. . .]

§ 62

Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 10, de 12 de enero de 2000
Última modificación: 4 de septiembre de 2018
Referencia: BOE-A-2000-544

Téngase en cuenta que las referencias hechas al término "permiso" se entenderan hechas al término "autorización" según establece la disposición adicional única de la Ley Orgánica 14/2003, de 20 de noviembre. Ref. BOE-A-2003-21187.

[. . .]

TÍTULO II

Régimen jurídico de los extranjeros

CAPÍTULO I

De la entrada y salida del territorio español

Artículo 25. *Requisitos para la entrada en territorio español.*

1. El extranjero que pretenda entrar en España deberá hacerlo por los puestos habilitados al efecto, hallarse provisto del pasaporte o documento de viaje que acredite su identidad, que se considere válido para tal fin en virtud de convenios internacionales suscritos por España y no estar sujeto a prohibiciones expresas. Asimismo, deberá presentar los documentos que se determinen reglamentariamente que justifiquen el objeto y condiciones de estancia, y acreditar medios de vida suficientes para el tiempo que pretenda permanecer en España, o estar en condiciones de obtener legalmente dichos medios.

2. Salvo en los casos en que se establezca lo contrario en los convenios internacionales suscritos por España o en la normativa de la Unión Europea, será preciso, además, un visado.

No será exigible el visado cuando el extranjero se encuentre provisto de la tarjeta de identidad de extranjero o, excepcionalmente, de una autorización de regreso.

3. Lo dispuesto en los párrafos anteriores no será de aplicación a los extranjeros que soliciten acogerse al derecho de asilo en el momento de su entrada en España, cuya concesión se regirá por lo dispuesto en su normativa específica.

4. Se podrá autorizar la entrada en España de los extranjeros que no reúnan los requisitos establecidos en los párrafos anteriores cuando existan razones excepcionales de índole humanitaria, interés público o cum plimiento de compromisos adquiridos por España. En estos casos, se procederá a hacer entrega al extranjero de la documentación que se establezca reglamentariamente.

5. La entrada en territorio nacional de los extranjeros a los que no les sea de aplicación el régimen comunitario, podrá ser registrada por las autoridades españolas a los efectos de control de su período de permanencia legal en España, de conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

[. . .]

Artículo 28. *De la salida de España.*

1. Las salidas del territorio español podrán realizarse libremente, excepto en los casos previstos en el Código Penal y en la presente Ley. La salida de los extranjeros a los que no les sea de aplicación el régimen comunitario, podrá ser registrada por las autoridades españolas a los efectos de control de su período de permanencia legal en España de conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Excepcionalmente, el Ministro del Interior podrá prohibir la salida del territorio español por razones de seguridad nacional o de salud pública. La instrucción y resolución de los expedientes de prohibición tendrá siempre carácter individual.

3. La salida será obligatoria en los siguientes supuestos:

a) Expulsión del territorio español por orden judicial, en los casos previstos en el Código Penal.

b) Expulsión o devolución acordadas por resolución administrativa en los casos previstos en la presente Ley.

c) Denegación administrativa de las solicitudes formuladas por el extranjero para continuar permaneciendo en territorio español, o falta de autorización para encontrarse en España.

d) Cumplimiento del plazo en el que un trabajador extranjero se hubiera comprometido a regresar a su país de origen en el marco de un programa de retorno voluntario.

[. . .]

Disposición adicional quinta. *Acceso a la información, colaboración entre Administraciones públicas y gestión informática de los procedimientos.*

1. En el cumplimiento de los fines que tienen encomendadas, y con pleno respeto a la legalidad vigente, las Administraciones públicas, dentro de su ámbito competencial, colaborarán en la cesión de datos relativos a las personas que sean consideradas interesados en los procedimientos regulados en esta Ley Orgánica y sus normas de desarrollo.

2. Para la exclusiva finalidad de cumplimentar las actuaciones que los órganos de la Administración General del Estado competentes en los procedimientos regulados en esta Ley Orgánica y sus normas de desarrollo tienen encomendadas, la Agencia Estatal de Administración Tributaria, la Tesorería General de la Seguridad Social y el Instituto Nacional de Estadística, este último en lo relativo al Padrón Municipal de Habitantes, facilitarán a aquéllos el acceso directo a los ficheros en los que obren datos que hayan de constar en dichos expedientes, y sin que sea preciso el consentimiento de los interesados, de acuerdo con la legislación sobre protección de datos.

Igualmente, los anteriores organismos facilitarán a las Comunidades Autónomas la información necesaria para ejercer sus competencias sobre autorizaciones iniciales de trabajo sin que tampoco sea preciso el consentimiento de los interesados.

3. La tramitación de los procedimientos en materia de extranjería derivados del cumplimiento de lo dispuesto en la presente Ley Orgánica, se realizará sobre una aplicación informática común cuya implantación y coordinación respecto de los restantes Departamentos implicados corresponderá al Ministerio de Trabajo e Inmigración. Dicha aplicación, garantizando la protección de datos de carácter personal, registrará la información y datos relativos a los extranjeros y ciudadanos de la Unión Europea residentes en España y sus autorizaciones, impulsará el cumplimiento de lo establecido por la legislación en materia de acceso electrónico de los ciudadanos a los servicios públicos y permitirá el conocimiento, en tiempo real, de la situación de las solicitudes de autorización reguladas en esta Ley por parte de los órganos administrativos que sean competentes en cada una de las fases del mismo, así como su intervención en la fase que recaiga dentro de su ámbito de competencias. Asimismo, la aplicación informática permitirá la generación de bases de datos estadísticas por las administraciones intervinientes para la obtención de la información actualizada y fiable sobre las magnitudes relativas a la inmigración y la extranjería.

En cumplimiento de lo establecido por la normativa comunitaria sobre la materia, la tramitación de procedimientos relativos a visados de tránsito y de estancia se realizará sobre la aplicación informática específicamente creada a los efectos, dependiente del Ministerio de Asuntos Exteriores y de Cooperación, que estará interconectada con la aplicación informática común, en orden a que en la base de datos de esta última conste información sobre los datos de los visados solicitados y concedidos en las Oficinas consulares o Misiones diplomáticas españolas en el exterior.

El Ministerio del Interior, de acuerdo con sus competencias en materia de orden público, seguridad pública y seguridad nacional, mantendrá un Registro central de extranjeros. Reglamentariamente, se establecerá la interconexión que, en su caso, resulte necesaria para que en la aplicación informática común conste la información que pueda repercutir en la situación administrativa de los extranjeros en España.

4. Cuando las Comunidades Autónomas, en el ámbito de sus competencias, intervengan en alguno de los procedimientos regulados en esta Ley, se garantizará que su participación en los procedimientos informatizados responda a estándares comunes que garanticen la necesaria coordinación de la actuación de todos los órganos administrativos intervinientes. Igualmente, la aplicación informática común dará acceso a las Comunidades Autónomas con competencias en materia de autorización de trabajo a la información necesaria para el ejercicio de sus competencias, entre la que se encontrará aquella relativa a la concesión y extinción de autorizaciones de reagrupación familiar concedidas en su territorio así como de las altas en Seguridad Social de las autorizaciones de trabajo iniciales concedidas por ellas.

5. El Observatorio Permanente de la Inmigración aunará el conjunto de la información estadística disponible en materia de extranjería, inmigración, protección internacional y nacionalidad, con independencia de la Administración Pública, Departamento ministerial u Organismo responsable de su elaboración, con la finalidad de servir como sistema de análisis e intercambio de la información cualitativa y cuantitativa relacionada con los movimientos migratorios al servicio de las entidades responsables de gestionar las políticas públicas en dichas materias.

[. . .]

§ 63

Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 186, de 5 de agosto de 1997
Última modificación: sin modificaciones
Referencia: BOE-A-1997-17574

[. . .]

Artículo 1. *Objeto.*

1. La presente Ley regula la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.

Asimismo, esta norma establece específicamente el régimen de garantías de los derechos fundamentales y libertades públicas de los ciudadanos que habrá de respetarse ineludiblemente en las sucesivas fases de autorización, grabación y uso de las imágenes y sonidos obtenidos conjuntamente por las videocámaras.

2. Las referencias contenidas en esta Ley a videocámaras, cámaras fijas y cámaras móviles se entenderán hechas a cualquier medio técnico análogo y, en general, a cualquier sistema que permita las grabaciones previstas en esta Ley.

Artículo 2. *Ámbito de aplicación.*

1. La captación, reproducción y tratamiento de imágenes y sonidos, en los términos previstos en esta Ley, así como las actividades preparatorias, no se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de lo establecido en el artículo 2.2 de la Ley Orgánica 1/1982, de 5 de mayo.

2. Sin perjuicio de las disposiciones específicas contenidas en la presente Ley, el tratamiento automatizado de las imágenes y sonidos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

[. . .]

Artículo 8. *Conservación de las grabaciones.*

1. Las grabaciones serán destruidas en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

2. Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas, siéndole de aplicación, en caso contrario, lo dispuesto en el artículo 10 de la presente Ley.

3. Se prohíbe la cesión o copia de las imágenes y sonidos obtenidos de conformidad con esta Ley, salvo en los supuestos previstos en el apartado 1 de este artículo.

4. Reglamentariamente la Administración competente determinará el órgano o autoridad gubernativa que tendrá a su cargo la custodia de las imágenes obtenidas y la responsabilidad sobre su ulterior destino, incluida su inutilización o destrucción. Dicho órgano será el competente para resolver sobre las peticiones de acceso o cancelación promovidas por los interesados.

[. . .]

Artículo 11. *Recursos.*

Contra las resoluciones dictadas en aplicación de lo previsto en esta Ley, cabrá la interposición de los recursos ordinarios en vía administrativa, contencioso-administrativa, así como los previstos en el artículo 53.2 de la Constitución, en los términos legalmente establecidos.

Disposición adicional primera.

Las Comunidades Autónomas con competencia para la protección de las personas y los bienes y para el mantenimiento del orden público, con arreglo a lo dispuesto en los correspondientes Estatutos de Autonomía, podrán dictar, con sujeción a lo prevenido en esta Ley, las disposiciones necesarias para regular y autorizar la utilización de videocámaras por sus fuerzas policiales y por las dependientes de las Corporaciones locales radicadas en su territorio, la custodia de las grabaciones obtenidas, la responsabilidad sobre su ulterior destino y las peticiones de acceso y cancelación de las mismas.

Cuando sean competentes para autorizar la utilización de videocámaras, las Comunidades Autónomas mencionadas en el párrafo anterior regularán la composición y el funcionamiento de la Comisión correspondiente, prevista en el artículo 3 de esta Ley, con especial sujeción a los principios de presidencia judicial y prohibición de mayoría de la Administración autorizante.

Disposición adicional segunda.

Cada autoridad competente para autorizar la instalación fija de videocámaras por parte de las Fuerzas y Cuerpos de Seguridad deberá crear un registro en el que consten todas las que haya autorizado.

[. . .]

Disposición adicional sexta.

Los propietarios y, en su caso, los titulares de derechos reales sobre los bienes afectados por las instalaciones reguladas en esta Ley, o quienes los posean por cualquier título, están obligados a facilitar y permitir su colocación y mantenimiento, sin perjuicio de la necesidad de obtener, en su caso, la autorización judicial prevista en el artículo 87.2 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y de las indemnizaciones que procedan según las leyes.

Disposición adicional séptima.

1. Se considerarán faltas muy graves en el régimen disciplinario de las Fuerzas y Cuerpos de Seguridad del Estado, las siguientes infracciones:

a) Alterar o manipular los registros de imágenes y sonidos siempre que no constituya delito.

b) Permitir el acceso de personas no autorizadas a las imágenes y sonidos grabados o utilizar éstos para fines distintos de los previstos legalmente.

c) Reproducir las imágenes y sonidos para fines distintos de los previstos en esta Ley.

d) Utilizar los medios técnicos regulados en esta Ley para fines distintos de los previstos en la misma.

2. Se considerarán faltas graves en el régimen disciplinario de las Fuerzas y Cuerpos de Seguridad del Estado las restantes infracciones a lo dispuesto en la presente Ley.

Disposición adicional octava.

La instalación y uso de videocámaras y de cualquier otro medio de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico se efectuará por la autoridad encargada de la regulación del tráfico a los fines previstos en el texto ar ticulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por Real Decreto legislativo 339/1990, de 2 de marzo, y demás normativa específica en la materia, y con sujeción a lo dispuesto en las Leyes Orgánicas 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, en el marco de los principios de utilización de las mismas previstos en esta Ley.

[. . .]

§ 64

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 157, de 2 de julio de 1985
Última modificación: 28 de octubre de 2015
Referencia: BOE-A-1985-12666

[. . .]

TÍTULO III

De las actuaciones judiciales

CAPÍTULO I

De la oralidad, publicidad y lengua oficial

[. . .]

Artículo 235 ter.

1. Es público el acceso a los datos personales contenidos en los fallos de las sentencias firmes condenatorias, cuando se hubieren dictado en virtud de los delitos previstos en los siguientes artículos:

a) Los artículos 305, 305 bis y 306 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
b) Los artículos 257 y 258 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, cuando el acreedor defraudado hubiese sido la Hacienda Pública.
c) El artículo 2 de la Ley Orgánica 12/1995, de 12 de diciembre, de Represión del Contrabando, siempre que exista un perjuicio para la Hacienda Pública estatal o de la Unión Europea.

2. En los casos previstos en el apartado anterior, el Letrado de la Administración de Justicia emitirá certificado en el que se harán constar los siguientes datos:

a) Los que permitan la identificación del proceso judicial.
b) Nombre y apellidos o denominación social del condenado y, en su caso, del responsable civil.
c) Delito por el que se le hubiera condenado.

d) Las penas impuestas.

e) La cuantía correspondiente al perjuicio causado a la Hacienda Pública por todos los conceptos, según lo establecido en la sentencia.

Mediante diligencia de ordenación el Letrado de la Administración de Justicia ordenará su publicación en el "Boletín Oficial del Estado".

3. Lo dispuesto en este artículo no será de aplicación en el caso de que el condenado o, en su caso, el responsable civil, hubiera satisfecho o consignado en la cuenta de depósitos y consignaciones del órgano judicial competente la totalidad de la cuantía correspondiente al perjuicio causado a la Hacienda Pública por todos los conceptos, con anterioridad a la firmeza de la sentencia.

[. . .]

Artículos 411 a 413.

(Suprimidos).

[. . .]

LIBRO VIII

Del Consejo General del Poder Judicial

TÍTULO I

De las atribuciones del Consejo General del Poder Judicial

[. . .]

Artículo 560.

1. El Consejo General del Poder Judicial tiene las siguientes atribuciones:

1.ª Proponer el nombramiento, en los términos previstos por la presente Ley Orgánica, del Presidente del Tribunal Supremo y del Consejo General del Poder Judicial.

2.ª Proponer el nombramiento de Jueces, Magistrados y Magistrados del Tribunal Supremo.

3.ª Proponer el nombramiento, en los términos previstos por la presente Ley Orgánica, de dos Magistrados del Tribunal Constitucional.

4.ª Ser oído por el Gobierno antes del nombramiento del Fiscal General del Estado.

5.ª Interponer el conflicto de atribuciones entre órganos constitucionales del Estado, en los términos previstos por la Ley Orgánica del Tribunal Constitucional.

6.ª Participar, en los términos legalmente previstos, en la selección de Jueces y Magistrados.

7.ª Resolver lo que proceda en materia de formación y perfeccionamiento, provisión de destinos, ascensos, situaciones administrativas y régimen disciplinario de Jueces y Magistrados.

8.ª Ejercer la alta inspección de Tribunales, así como la supervisión y coordinación de la actividad inspectora ordinaria de los Presidentes y Salas de Gobierno de los Tribunales.

9.ª Impartir instrucciones a los órganos de gobierno de Juzgados y Tribunales en materias de la competencia de éstos, así como resolver los recursos de alzada que se interpongan contra cualesquiera acuerdos de los mismos.

10.ª Cuidar de la publicación oficial de las sentencias y demás resoluciones que se determinen del Tribunal Supremo y del resto de órganos judiciales.

A tal efecto el Consejo General del Poder Judicial, previo informe de las Administraciones competentes, establecerá reglamentariamente el modo en que habrán de elaborarse los libros electrónicos de sentencias, la recopilación de las mismas, su tratamiento, difusión y certificación, para velar por su integridad, autenticidad y acceso, así como para asegurar el cumplimiento de la legislación en materia de protección de datos personales.

11.ª Regular la estructura y funcionamiento de la Escuela Judicial, así como nombrar a su Director y a sus profesores.

12.ª Regular la estructura y funcionamiento del Centro de Documentación Judicial, así como nombrar a su Director y al resto de su personal.

13.ª Nombrar al Vicepresidente del Tribunal Supremo, al Promotor de la Acción Disciplinaria y al Jefe de la Inspección de Tribunales.

14.ª Nombrar al Director del Gabinete Técnico del Consejo General del Poder Judicial.

15.ª Regular y convocar el concurso-oposición de ingreso en el Cuerpo de Letrados del Consejo General del Poder Judicial.

16.ª Ejercer la potestad reglamentaria, en el marco estricto de desarrollo de las previsiones de la Ley Orgánica del Poder Judicial, en las siguientes materias:

a) Organización y funcionamiento del Consejo General del Poder Judicial.

b) Personal del Consejo General del Poder Judicial en el marco de la legislación sobre la función pública.

c) Órganos de gobierno de Juzgados y Tribunales.

d) Publicidad de las actuaciones judiciales.

e) Publicación y reutilización de las resoluciones judiciales.

f) Habilitación de días y horas, así como fijación de horas de audiencia pública.

g) Constitución de los órganos judiciales fuera de su sede.

h) Especialización de órganos judiciales.

i) Reparto de asuntos y ponencias.

j) Régimen de guardias de los órganos jurisdiccionales.

k) Organización y gestión de la actuación de los órganos judiciales españoles en materia de cooperación jurisdiccional interna e internacional.

l) Establecimiento de las bases y estándares de compatibilidad de los sistemas informáticos que se utilicen en la Administración de Justicia.

m) Condiciones accesorias para el ejercicio de los derechos y deberes que conforman el estatuto de Jueces y Magistrados, así como el régimen jurídico de las Asociaciones judiciales, sin que tal desarrollo reglamentario pueda suponer innovación o alteración alguna de la regulación legal.

En ningún caso, las disposiciones reglamentarias del Consejo General del Poder Judicial podrán afectar o regular directa o indirectamente los derechos y deberes de personas ajenas al mismo.

17.ª Elaborar y ejecutar su propio presupuesto, en los términos previstos en la presente Ley Orgánica.

18.ª Aprobar la relación de puestos de trabajo del personal funcionario a su servicio.

19ª Colaborar con la Autoridad de Control en materia de protección de datos en el ámbito de la Administración de Justicia. Asimismo, asumirá las competencias propias de aquélla, únicamente respecto a la actuación de Jueces y Magistrados con ocasión del uso de ficheros judiciales.

20.ª Recibir quejas de los ciudadanos en materias relacionadas con la Administración de Justicia.

21.ª Elaborar y aprobar, conjuntamente con el Ministerio de Justicia y, en su caso, oídas las Comunidades Autónomas cuando afectare a materias de su competencia, los sistemas de racionalización, organización y medición de trabajo que se estimen convenientes para determinar la carga de trabajo que pueda soportar un órgano jurisdiccional.

La determinación de la carga de trabajo que cabe exigir, a efectos disciplinarios, al Juez o Magistrado corresponderá en exclusiva al Consejo General del Poder Judicial.

22.ª Proponer, previa justificación de la necesidad, las medidas de refuerzo que sean precisas en concretos órganos judiciales.

23.ª Emitir informe en los expedientes de responsabilidad patrimonial por anormal funcionamiento de la Administración de Justicia.

24.ª Aquellas otras que le atribuya la Ley Orgánica del Poder Judicial.

2. Los proyectos de reglamentos de desarrollo se someterán a informe de las asociaciones profesionales de Jueces y Magistrados y de las corporaciones profesionales o asociaciones de otra naturaleza que tengan reconocida legalmente representación de intereses a los que puedan afectar. Se dará intervención a la Administración del Estado, por medio del Ministerio de Justicia, y a las de las Comunidades Autónomas siempre que una y otras tengan competencias relacionadas con el contenido del reglamento o sea necesario coordinar éstas con las del Consejo General. Se recabarán las consultas y los estudios previos que se consideren pertinentes y un dictamen de legalidad sobre el proyecto.

En todo caso, se elaborará un informe previo de impacto de género.

El Ministerio Fiscal será oído cuando le afecte la materia sobre la que verse el proyecto y especialmente en los supuestos contemplados en las letras d) y f) a j) del apartado 1.16.ª de este artículo.

3. A los efectos de lo previsto en la letra l) del apartado 1.16.ª de este artículo, el Consejo General del Poder Judicial someterá a la aprobación del Comité Técnico Estatal de la Administración judicial electrónica la definición y validación funcional de los programas y aplicaciones informáticos estableciendo a nivel estatal los modelos de resoluciones, procedimientos e hitos clave de la gestión procesal.

En todo caso, la implementación técnica de todas estas medidas en los programas y aplicaciones informáticas corresponderá al Ministerio de Justicia y demás administraciones con competencias sobre los medios materiales al servicio de la Administración de Justicia.

4. Cuando en el ejercicio de las atribuciones legalmente previstas en este artículo el Consejo General del Poder Judicial adopte medidas que comporten un incremento de gasto, será preciso informe favorable de la Administración competente que deba soportar dicho gasto.

[. . .]