Tema 8

La protección de datos personales y su régimen Jurídico: principios, derechos, responsable y encargado del tratamiento, delegado y autoridades de protección de datos. Derechos digitales.

ÍNDICE

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el **artículo 18.4 de la Constitución española**. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «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».

A nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho a 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. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa.

Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva.

El Reglamento general de protección de datos pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora 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 esos datos. La transposición de la directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos.

A nivel estatal cabe destacar la **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.** La norma se compone de un total de 10 títulos. Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier 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. Esta ley orgánica no será de aplicación:

a) A los **tratamientos excluidos** del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.
b) A los **tratamientos de datos de personas fallecidas**, sin perjuicio de las especialidades que veremos.
c) A los **tratamientos sometidos a la normativa sobre protección de materias clasificadas**.

Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, **se regirán por lo dispuesto en su legislación específica** si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles.

El tratamiento de datos llevado a cabo con ocasión de la tramitación por los **órganos judiciales de los procesos de los que sean competentes**, así como el realizado dentro de la gestión de la Oficina Judicial, se **regirán por lo dispuesto en el Reglamento (UE) 2016/679** y la presente ley orgánica, sin perjuicio de las disposiciones de la **Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables.**

El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la Oficina Fiscal, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de las normas procesales que le sean aplicables.

1. Introducción

El **nuevo Reglamento General de Protección de Datos (RGPD) entró en vigor en mayo de 2016 y será aplicable a partir de mayo de 2018.** En este periodo transitorio y aun cuando siguen vigentes las disposiciones de la Directiva 95/46 y las correspondientes normas nacionales de desarrollo, los responsables y encargados de tratamiento deben ir preparando y adoptando las medidas necesarias para estar en condiciones de cumplir con las previsiones del RGPD en el momento en que sea de aplicación. El RGPD es una norma directamente aplicable, que no requiere de normas internas de trasposición ni tampoco, en la mayoría de los casos, de normas de desarrollo o aplicación. Por ello, los responsables deben ante todo asumir que la norma de referencia es el RGPD y no las normas nacionales, como venía sucediendo hasta ahora con la Directiva 95/46.

El RGPD señala que las medidas dirigidas a garantizar su cumplimiento 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. De acuerdo con este enfoque, algunas de las medidas que el RGPD establece se aplicarán sólo cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten. La aplicación de las medidas previstas por el RGPD debe adaptarse, por tanto, a las características de las organizaciones. Lo que puede ser adecuado para una organización que maneja datos de millones de interesados en tratamientos complejos que involucran información personal sensible o volúmenes importantes de datos sobre cada afectado no es necesario para una pequeña empresa que lleva a cabo un volumen limitado de tratamientos de datos no sensibles.

1.1. Tratamiento que no requiere identificación

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.**

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 (derechos),

excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación

1.2. Datos de las personas fallecidas.

Las **personas vinculadas** al fallecido por **razones familiares** o de **hecho** así como sus **herederos** podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, **su rectificación o supresión.**

Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, **cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.**

> Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, **el acceso a los datos personales de este y, en su caso su rectificación o supresión.**

Mediante **real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones** y, en su caso, el registro de los mismos.

En **caso de fallecimiento de menores**, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

En caso de fallecimiento de **personas con discapacidad**, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

1.3. Tratamiento basado en el consentimiento del afectado.

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**

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.

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.

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.

De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda **manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.**

Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

1.4. Consentimiento de los menores de edad.

El RGPD habilita a los Estados miembros de la Unión Europea a establecer por ley una edad inferior a 16 años para considerar lícito el tratamiento de sus datos basado en su consentimiento, siempre y cuando dicha edad no fuera inferior a 13 años.

El tratamiento de los datos personales de un menor de edad **únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.**

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

1.5. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.

El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c)[1] del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o **una norma con rango de ley**, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e)[2] del Reglamento (UE) 2016/679, cuando derive de una competencia **atribuida por una norma con rango de ley**.

1.6. Categorías especiales de datos.

El artículo 9.1 RGPD señala que **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 las orientación sexuales de una persona física.

[1] El tratamiento será lícito si es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.
[2] El tratamiento será lícito si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

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.

A los efectos del artículo 9.2.a)[3] del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, **el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.**

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

[3] 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;

1.7. Tratamiento de datos de naturaleza penal.

El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.

El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.

Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

2. Principios

Estos principios se encuentran recogidos en el **artículo 5 del RGPD** y supone que 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**»).

Además, el responsable del tratamiento será responsable del cumplimiento de estos principios y deberá ser capaz de demostrarlo («**responsabilidad proactiva»).**

3. Derechos

3.1. Derecho de acceso

El derecho de acceso es tu derecho a dirigirte al responsable del tratamiento para conocer si está tratando o no tus datos de carácter personal y, en el caso de que se esté realizando dicho tratamiento, obtener la siguiente información:

- Una copia de tus datos personales que son objeto del tratamiento
- Los fines del tratamiento
- Las categorías de datos personales que se traten

- Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular, los destinatarios en países terceros u organizaciones internacionales

- El plazo previsto de conservación de los datos personales, o si no es posible, los criterios utilizados para determinar este plazo

- La existencia del derecho del interesado a solicitar al responsable: la rectificación o supresión de sus datos personales, la limitación del tratamiento de sus datos personales u oponerse a ese tratamiento

- El derecho a presentar una reclamación ante una Autoridad de Control

- Cuando los datos personales no se hayan obtenido directamente de ti, cualquier información disponible sobre su origen

- La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y al menos en tales casos, información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de ese tratamiento para el interesado

- Cuando se transfieran datos personales a un tercer país o a una organización internacional, tienes derecho a ser informado de las garantías adecuadas en las que se realizan las transferencias

3.2. Derecho de rectificación

El ejercicio de este derecho supone que podrás obtener la rectificación de tus datos personales que sean inexactos sin dilación indebida del responsable del tratamiento.

Teniendo en cuenta los fines del tratamiento, tienes derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

En tu solicitud deberás indicar a qué datos te refieres y la corrección que hay que realizar. Además, cuando sea necesario, deberás acompañar tu solicitud de la documentación que justifique la inexactitud o el carácter incompleto de tus datos.

3.3. Derecho de oposición

Este derecho, como su nombre indica, supone que te puedes oponer a que el responsable realice un tratamiento de los datos personales en los siguientes supuestos:

Cuando sean objeto de tratamiento basado en una misión de interés público o en el interés legítimo, incluido la elaboración de perfiles:

- El responsable dejará de tratar los datos salvo que acredite motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones

Cuando el tratamiento tenga como finalidad la mercadotecnia directa, incluida también la elaboración de perfiles anteriormente citada:

- Ejercitado este derecho para esta finalidad, los datos personales dejarán de ser tratados para dichos fines

3.4. Derecho de supresión (“al olvido”)

Podrás ejercitar este derecho ante la persona responsable solicitando la supresión de sus datos de carácter personal cuando concurra alguna de las siguientes circunstancias:

- Si tus datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo

- Si el tratamiento de tus datos personales se ha basado en el consentimiento que prestaste a la personaresponsable, y retiras el mismo, siempre que el citado tratamiento no se base en otra causa que lo legitime

- Si te has opuesto al tratamiento de tus datos personales al ejercitar el derecho de oposición en las siguientes circunstancias:

    - El tratamiento de la persona responsable se fundamentaba en el interés legítimo o en el cumplimiento de una misión de interés público, y no han prevalecido otros motivos para legitimar el tratamiento de tus datos

- A que tus datos personales sean objeto de mercadotecnia directa, incluyendo la elaboración perfiles relacionada con la citada mercadotecnia

- Si tus datos personales han sido tratados ilícitamente

- Si tus datos personales deben suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique a la persona responsable del tratamiento

- Si los datos personales se han obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1 (condiciones aplicables al tratamiento de datos de los menores en relación con los servicios de la sociedad de la información).

Además, el RGPD al regular este derecho lo conecta de cierta forma con el denominado "derecho al olvido", de manera que este derecho de supresión se amplíe de tal forma que la persona 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.

No obstante, este derecho no es ilimitado, de tal forma que puede ser factible no proceder a la supresión cuando el tratamiento sea necesario 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 a la persona responsable, por razones de interés público, en el ámbito de la salud pública, con fines de archivo de interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

3.5. Derecho a la limitación del tratamiento

Este nuevo derecho consiste en que obtengas la limitación del tratamiento de tus datos que realiza el responsable, si bien su ejercicio presenta dos vertientes:

Puedes solicitar la suspensión del tratamiento de tus datos:

- Cuando impugnes la exactitud de tus datos personales, durante un plazo que permita al responsable su verificación

- Cuando te hayas opuesto al tratamiento de tus datos personales que el responsable realiza en base al interés legítimo o misión de interés público, mientras aquel verifica si estos motivos prevalecen sobre los tuyos

Solicitar al responsable la conservación tus datos:

- Cuando el tratamiento sea ilícito y te has opuesto a la supresión de tus datos y en su lugar solicitas la limitación de su uso

- Cuando 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

3.6. Derecho a la portabilidad

La finalidad de este nuevo derecho es reforzar aún más el control de tus datos personales, de forma que cuando el tratamiento se efectúe por medios automatizados, recibas tus datos personales en un formato estructurado, de uso común, de lectura mecánica e interoperable, y puedas transmitirlos a otro responsable del tratamiento, siempre que el tratamiento se legitime en base al consentimiento o en el marco de la ejecución de un contrato.

No obstante, este derecho, por su propia naturaleza, no se puede aplicar cuando el tratamiento sea necesario para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable.

3.7. Derecho a no ser objeto de decisiones individuales automatizadas

Este derecho pretende garantizar que no seas objeto de una decisión basada únicamente en el tratamiento de tus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre ti o te afecte significativamente de forma similar.

Sobre esta elaboración de perfiles, se trata de cualquier forma de tratamiento de tus datos personales que evalúe aspectos personales, en particular analizar o predecir aspectos relacionados con tu rendimiento en el trabajo, situación económica, salud, las preferencias o intereses personales, fiabilidad o el comportamiento.

No obstante, este derecho no será aplicable cuando:

- Sea necesario para la celebración o ejecución de un contrato entre tú y el responsable
- El tratamiento de tus datos se fundamente en tu consentimiento prestado previamente

No obstante, en estos dos primeros supuestos, el responsable debe garantizar tu derecho a obtener la intervención humana, expresar tu punto de vista e impugnar la decisión.

- Esté autorizado por el Derecho de la Unión o de los Estados miembros y se establezcan medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos del interesado.

A su vez, estas excepciones no se aplicarán sobre las categorías especiales de datos (art.9.1), salvo que se aplique el artículo 9.2.letra a) o g) y se hayan tomado las medidas adecuadas citadas en el párrafo anterior.

3.8. Derecho de información

Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

La información básica a la que se refiere el apartado anterior deberá contener, al menos:

a) La identidad del responsable del tratamiento y de su representante, en su caso.
b) La finalidad del tratamiento.
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

En estos supuestos, la información básica incluirá también:

a) Las categorías de datos objeto de tratamiento.
b) Las fuentes de las que procedieran los datos.

4. Delegado de protección de datos

4.1. Designación de un delegado de protección de datos.

Según el artículo 37 del RGPD 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 personales** con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

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.

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.

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.

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.

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.

Por su parte, el artículo 34 de la LOPDGDD señala que los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

a) Los **colegios profesionales y sus consejos generales**.
b) Los **centros docentes** que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
c) Las **entidades que exploten redes y presten servicios de comunicaciones electrónicas** conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
d) Los **prestadores de servicios de la sociedad de la información** cuando elaboren a gran escala perfiles de los usuarios del servicio.
e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, **supervisión y solvencia de entidades de crédito**.
f) Los establecimientos **financieros de crédito**.
g) Las entidades **aseguradoras y reaseguradoras**.
h) Las **empresas de servicios de inversión**, reguladas por la **legislación del Mercado de Valores**.
i) Los **distribuidores y comercializadores de energía eléctrica y los distribuidores** y comercializadores de gas natural.
j) Las **entidades responsables de ficheros comunes** para la evaluación de la solvencia **patrimonial y crédito** o de los ficheros comunes para la gestión y prevención del fraude,

incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

k) Las **entidades que desarrollen actividades de publicidad y prospección comercial**, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los **centros sanitarios** legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las **entidades que tengan como uno de sus objetos la emisión de informes comerciales** que puedan referirse a personas físicas.

n) Los **operadores que desarrollen la actividad de juego a través de canales electrónicos**, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

o) Las **empresas de seguridad privada.**

p) Las **federaciones deportivas** cuando traten datos de menores de edad.

Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

4.2. Cualificación del delegado de protección de datos.

El cumplimiento de los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a **través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.**

4.3. Posición del delegado de protección de datos.

El delegado de protección de datos actuará **como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos.** El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.

Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.

Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

4.4. Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.

Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación

contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.

En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.

Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

4.5. Funciones

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 cumplimient**o 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.

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.

5. Responsable vs. encargado del tratamiento

5.1. Responsable

5.1.1. Concepto

El **«responsable del tratamiento» o «responsable»** es 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.

El **responsable del tratamiento** determina los **fines** y los **medios** relacionados con el tratamiento de los datos personales. De modo que, si decide «por qué» y «cómo» deberán tratarse los datos personales, usted es el responsable del tratamiento. Los empleados que realizan el tratamiento de los datos personales en su organización lo hacen en cumplimiento de las funciones que usted ejerce como responsable del tratamiento.

5.1.2. Funciones

Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones 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, moral o social significativo para los afectados.
b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.
c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.
d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.
e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.
f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.
g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.
h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

5.1.3. Bloqueo de datos

El responsable del tratamiento **estará obligado a bloquear los datos** cuando proceda a su rectificación o supresión.

El **bloqueo de los datos** consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Transcurrido **ese plazo deberá procederse a la destrucción de los datos.**

Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.

Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.

La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, dentro del ámbito de sus respectivas competencias, podrán fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

5.2. Encargado del tratamiento

Por su parte, el «encargado del tratamiento» o «encargado» **es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;**

El **encargado del tratamiento trata los datos personales** únicamente **por cuenta del responsable del tratamiento**. El encargado del tratamiento de los datos suele ser un tercero externo a la empresa; sin embargo, en el caso de los grupos de empresas, una de ellas puede actuar como encargada del tratamiento para otra.

Las obligaciones del encargado del tratamiento con respecto al responsable deberán especificarse en un contrato u otro acto jurídico. Por ejemplo, el contrato debe indicar lo que pasará con los datos personales una vez finalizado el contrato. Una actividad típica de los encargados es ofrecer soluciones informáticas, como almacenamiento en la nube. El encargado del tratamiento solo puede subcontratar una parte de esta tarea a otro encargado o designar un coencargado cuando haya recibido la autorización previa por escrito del responsable del tratamiento.

El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.

Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado.

No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

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

En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma

reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

5.3. Diferencias y ejemplos

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.

Cuando sean proporcionadas en relación con las actividades de tratamiento, se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

La adhesión a códigos de conducta aprobados o a un mecanismo de certificación podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Ejemplos

Responsable y encargado del tratamiento

Una cervecería que tiene muchos empleados firma un contrato con una empresa de nóminas, para poder pagarles los salarios. La cervecería indica a la empresa de nóminas cuándo deben pagarse las nóminas, cuándo un empleado abandona la empresa o si tiene un aumento de sueldo, y proporciona toda la demás información sobre la nómina y el pago. La empresa de nóminas proporciona el sistema informático y conserva los datos de los empleados. La cervecería es el responsable del tratamiento y la empresa de nóminas es el encargado del tratamiento.

Corresponsables del tratamiento

Su empresa presta servicios de guardería a través de una plataforma por internet. Al mismo tiempo, la empresa tiene un contrato con otra empresa que le permite ofrecer servicios de valor añadido. Esos servicios incluyen la posibilidad de que los padres no solo elijan la canguro, sino también que alquilen juegos y DVD que esta puede traer. Ambas empresas participan en los aspectos técnicos del sitio web. En este caso, las dos empresas han decidido utilizar la plataforma

para ambos fines (servicios de guardería y alquiler de DVD o juegos) y a menudo compartirán los nombres de sus clientes. Por tanto, ambas empresas son corresponsables del tratamiento, porque no solo están de acuerdo en ofrecer la posibilidad de «servicios combinados», sino que también diseñan y utilizan una plataforma común.

5.4. Protección de datos desde el diseño y por defecto

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.

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.

6. La Agencia Española de Protección de Datos

6.1. Naturaleza jurídica

La Agencia Española de Protección de Datos es una **autoridad administrativa independiente** de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será «**Agencia Española de Protección de Datos, Autoridad Administrativa Independiente».**

Se relaciona con el **Gobierno** a través del **Ministerio de Justicia**.

La Agencia Española de Protección de Datos tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos.

La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y en su caso, la Fiscalía General del Estado, **colaborarán** en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

La Agencia Española de Protección de Datos se rige por **lo dispuesto en el Reglamento (UE) 2016/679, la LOPDGDD y sus disposiciones de desarrollo.**

Supletoriamente, en cuanto sea compatible con su plena independencia y sin perjuicio de lo previsto en el artículo 63.2 de esta ley orgánica, se regirá por las normas citadas en el artículo 110.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

El Gobierno, a propuesta de la Agencia Española de Protección de Datos, aprobará su Estatuto mediante real decreto (**Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos).**

6.2. Presidencia

La Presidencia de la Agencia Española de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices.

La Presidencia de la Agencia Española de Protección de Datos estará auxiliada por **un Adjunto** en el que podrá delegar sus funciones, a excepción de las relacionadas con los procedimientos en caso de posible vulneración de la normativa de protección de datos, y que la sustituirá en el ejercicio de las mismas en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Ambos ejercerán sus funciones con ple**na independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño.** Les será aplicable la legislación reguladora del ejercicio del alto cargo de la Administración General del Estado.

En los supuestos de ausencia, vacante o enfermedad de la persona titular de la Presidencia o cuando concurran en ella alguno de los motivos de abstención o recusación previstos en el

artículo 23 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el ejercicio de las competencias relacionadas con los procedimientos en caso de posible vulneración de la normativa de protección de datos serán asumidas por la persona titular del órgano directivo que desarrolle las funciones de inspección. En el supuesto de que cualquiera de las circunstancias mencionadas concurriera igualmente en dicha persona, el ejercicio de las competencias afectadas será asumido por las personas titulares de los órganos directivos con nivel de subdirección general, por el orden establecido en el Estatuto.

El ejercicio del resto de competencias será asumido por el Adjunto en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos y, en su defecto, por las personas titulares de los órganos directivos con nivel de subdirección general, por el orden establecido en el Estatuto.

Presidencia de la Agencia Española de Protección de Datos y su Adjunto serán nombrados por el Gobierno, a propuesta del Ministerio de Justicia, **entre personas de reconocida competencia profesional, en particular en materia de protección de datos.**

Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Justicia ordenará la publicación en el Boletín Oficial del Estado de la convocatoria pública de candidatos.

Previa evaluación del mérito, capacidad, competencia e idoneidad de los candidatos, **el Gobierno remitirá al Congreso de los Diputados una propuesta de Presidencia y Adjunto acompañada de un informe justificativo** que, tras la celebración de la preceptiva audiencia de los candidatos, deberá ser ratificada por la Comisión de Justicia en votación pública por mayoría de **tres quintos de sus miembros en primera votación** o, de no alcanzarse ésta, por mayoría **absoluta en segunda votación**, que se realizará inmediatamente después de la primera. En este último supuesto, los votos favorables deberán proceder de Diputados pertenecientes, al menos, a dos grupos parlamentarios diferentes.

La Presidencia y el Adjunto de la Agencia Española de Protección de Datos **serán nombrados por el Consejo de Ministros mediante real decreto.**

El mandato de la Presidencia y del Adjunto de la Agencia Española de Protección de Datos tiene una duración de **cinco años y puede ser renovado para otro período de igual duración**.

La Presidencia y el Adjunto solo cesarán antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Ministros, por:

a) Incumplimiento grave de sus obligaciones,
b) incapacidad sobrevenida para el ejercicio de su función,
c) incompatibilidad, o
d) condena firme por delito doloso.

En los supuestos previstos en las letras a), b) y c) será necesaria la ratificación de la separación por las mayorías parlamentarias previstas en el apartado 3 de este artículo.

Los actos y disposiciones dictados por la Presidencia de la Agencia Española de Protección de Datos ponen fin a la vía **administrativa, siendo recurribles, directamente, ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.**

6.3. Consejo Consultivo

La Presidencia de la Agencia Española de Protección de Datos estará asesorada por un Consejo Consultivo compuesto por los siguientes miembros:

a) Un **Diputado**, propuesto por el Congreso de los Diputados.
b) Un **Senador**, propuesto por el Senado.
c) Un representante designado por el **Consejo General del Poder Judicial**.
d) Un representante de la **Administración General del Estado** con experiencia en la materia, propuesto por el Ministro de Justicia.
e) Un representante de **cada Comunidad Autónoma** que haya creado una Autoridad de protección de datos en su ámbito territorial, propuesto de acuerdo con lo que establezca la respectiva Comunidad Autónoma.
f) Un experto propuesto por la **Federación Española de Municipios y Provincias**.
g) Un experto propuesto por el **Consejo de Consumidores y Usuarios**.
h) Dos expertos propuestos por **las Organizaciones Empresariales.**
i) Un representante de los **profesionales de la protección de datos y de la privacidad**, propuesto por la asociación de ámbito estatal con mayor número de asociados.
j) Un representante de los organismos o entidades de supervisión y resolución extrajudicial de conflictos previstos en el Capítulo IV del Título V, propuesto por el Ministro de Justicia.
k) Un experto, propuesto por la **Conferencia de Rectores de las Universidades Españolas.**

l) Un representante de las organizaciones que agrupan a los **Consejos Generales, Superiores** y **Colegios Profesionales** de ámbito estatal de las diferentes **profesiones colegiadas,** propuesto por el Ministro de Justicia.

m) Un representante de los **profesionales de la seguridad de la información**, propuesto por la asociación de ámbito estatal con mayor número de asociados.

n) Un experto en **transparencia y acceso a la información pública** propuesto por el Consejo de Transparencia y Buen Gobierno.

o) Dos expertos propuestos por las **organizaciones sindicales** más representativas.

A los efectos del apartado anterior, la condición de experto requerirá acreditar conocimientos especializados en el Derecho y la práctica en materia de protección de datos mediante el ejercicio profesional o académico.

Los miembros del Consejo Consultivo serán nombrados por **orden del Ministro de Justicia**, publicada en el Boletín Oficial del Estado.

El Consejo Consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia Española de Protección de Datos y, en todo caso, una vez al semestre.

Las decisiones tomadas por el Consejo Consultivo no tendrán en ningún caso carácter vinculante.

En todo lo no previsto por esta ley orgánica, el régimen, competencias y funcionamiento del Consejo Consultivo serán los establecidos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

6.4. Potestades

6.4.1. Potestades de investigación

La Agencia Española de Protección de Datos desarrollará su actividad de investigación a través de las actuaciones previstas en el Título VIII y de los planes de auditoría preventivas.

6.4.2. Planes de auditoría

La Presidencia de la Agencia Española de Protección de Datos podrá acordar la realización de planes de **auditoría preventiva**, referidos a los tratamientos de un sector concreto de actividad. Tendrán por objeto el análisis del cumplimiento de las disposiciones del Reglamento (UE) 2016/679 y de la presente ley orgánica, a partir de la realización de actividades de investigación

sobre entidades pertenecientes al sector inspeccionado o sobre los responsables objeto de la auditoría.

A resultas de los planes de auditoría, la **Presidencia de la Agencia Española de Protección de Datos podrá dictar las directrices generales o específicas para un concreto responsable o encargado** de los tratamientos precisas para asegurar la plena adaptación del sector o responsable al Reglamento (UE) 2016/679 y a la presente ley orgánica.

En la elaboración de dichas directrices la Presidencia de la Agencia Española de Protección de Datos podrá solicitar la colaboración de los organismos de supervisión de los códigos de conducta y de resolución extrajudicial de conflictos, si los hubiere.

Las directrices serán de obligado cumplimiento para el sector o responsable al que se refiera el plan de auditoría

6.4.3. Potestades de regulación.

La Presidencia de la Agencia Española de Protección de Datos podrá dictar disposiciones que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, que se denominarán «**Circulares de la Agencia Española de Protección de Datos».**

elaboración se sujetará al procedimiento establecido en el Estatuto de la Agencia Española de Protección de Datos, que deberá prever los informes técnicos y jurídicos que fueran necesarios y la audiencia a los interesados.

Las circulares serán obligatorias una vez publicadas en el Boletín Oficial del Estado.

6.4.4. Acción exterior.

Corresponde **a la Agencia Española de Protección de Datos la titularidad y el ejercicio de las funciones relacionadas con la acción exterior del Estado en materia de protección de datos**.

Asimismo a las comunidades autónomas, a través de las autoridades autonómicas de protección de datos, les compete ejercitar las funciones como sujetos de la acción exterior en el marco de sus competencias de conformidad con lo dispuesto en la Ley 2/2014, de 25 de marzo, de la Acción y del Servicio Exterior del Estado, así como celebrar acuerdos internacionales administrativos en ejecución y concreción de un tratado internacional y acuerdos no normativos con los órganos análogos de otros sujetos de derecho internacional, no vinculantes

jurídicamente para quienes los suscriben, sobre materias de su competencia en el marco de la Ley 25/2014, de 27 de noviembre, de Tratados y otros Acuerdos Internacionales.

La **Agencia Española de Protección de Datos es el organismo competente para la protección de las personas físicas en lo relativo al tratamiento de datos personales derivado de la aplicación de cualquier Convenio Internaciona**l en el que sea parte el Reino de España que atribuya a una autoridad nacional de control esa competencia y la representante común de las autoridades de Protección de Datos en el Comité Europeo de Protección de Datos, conforme a lo dispuesto en el artículo 68.4 del Reglamento (UE) 2016/679.

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.

Sin perjuicio de lo dispuesto en el apartado 1, la Agencia Española de Protección de Datos:

a) Participará en **reuniones y foros internacionales** de ámbito distinto al de la Unión Europea establecidos de común acuerdo por las autoridades de control independientes en materia de protección de datos.
b) Participará, como autoridad española, en las **organizaciones internacionales** competentes en materia de protección de datos, en los comités o grupos de trabajo, de estudio y de colaboración de organizaciones internacionales que traten materias que afecten al derecho fundamental a la protección de datos personales y en otros foros o grupos de trabajo internacionales, en el marco de la acción exterior del Estado.
c) **Colaborará con autoridades, instituciones, organismos y Administraciones de otros Estados** a fin de impulsar, promover y desarrollar el derecho fundamental a la protección de datos, en particular en el ámbito iberoamericano, pudiendo suscribir acuerdos internacionales administrativos y no normativos en la materia.

7. Derechos Digitales

Regulados en el **Título X de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales** y también en la **Carta de Derechos Digitales.**

7.1. La Carta de Derechos Digitales

La Carta de Derechos Digitales española es un documento elaborado por el Ministerio de Asuntos Económicos y Transformación Digital de España con el objetivo de establecer un conjunto de derechos que protejan los intereses y las libertades de los ciudadanos en el ámbito digital, garantizando su privacidad y seguridad en internet, así como su derecho a la neutralidad de la red y a una educación digital adecuada. **Fue aprobada por el Gobierno español el 14 de julio de 2021 y no tiene fuerza obligatoria.**

Esta se inspira en la Carta de Derechos Fundamentales de la Unión Europea y en la Declaración Universal de Derechos Humanos de las Naciones Unidas. Además, se enmarca en el contexto de la estrategia digital de España y de la Unión Europea, que buscan fomentar la innovación y el desarrollo tecnológico, al mismo tiempo que garantizan la protección de los derechos de los ciudadanos.

La Carta se divide en **27 derechos, agrupados en 6 categorías:**

1. **Derechos de libertad (I - VII):** protege y garantiza la libertad de expresión, privacidad y seguridad en el entorno digital. Reconoce el derecho de las personas a expresar sus ideas y opiniones sin censura, salvaguardando su privacidad y estableciendo medidas para prevenir el acoso en línea y otros comportamientos perjudiciales.

2. **Derechos de igualdad (VIII - XII):** busca garantizar la igualdad de oportunidades y trato en el entorno digital. Se enfoca en promover la inclusión digital, eliminar la brecha digital y garantizar el acceso equitativo a la tecnología y a los servicios digitales.

3. **Derechos de participación y de conformación del espacio público (XIII - XVIII):** promueve la participación ciudadana activa y la conformación de un espacio público digital inclusivo y respetuoso. Busca garantizar el acceso y la participación igualitaria de los ciudadanos en los procesos de toma de decisiones públicas a través de medios digitales, fomentando la transparencia y la colaboración.

4. **Derechos del entorno laboral y empresarial (XIX - XX):** garantiza los derechos de los trabajadores y establece responsabilidades para las empresas en el ámbito digital. Busca proteger la privacidad de los trabajadores, regular el teletrabajo y promover un entorno laboral digital saludable.

5. **Derechos digitales en entornos específicos (XXI - XXVI):** protege y garantiza los derechos en diversos entornos como el acceso a datos con fines de investigación, derechos ante la inteligencia artificial o la libertad de creación y acceso a la cultura en el entorno digital.

6. **Garantías (XXVII- XXVIII):** establece las medidas necesarias para asegurar la efectividad de los derechos digitales establecidos. Busca promover mecanismos de supervisión, cumplimiento y sanción, así como fortalecer las autoridades competentes en la protección de los derechos digitales.

7.2. Título X LOPDGDD

Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. **Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación.**

7.2.1. Derecho a la neutralidad de Internet.

Los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.

7.2.2. Derecho de acceso universal a Internet.

Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica.

Se **garantizará** un acceso universal, asequible, de calidad y no discriminatorio para toda la población.

El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral.

El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores.

La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales.

El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales.

7.2.3. Derecho a la seguridad digital.

Los **usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet**. Los proveedores de **servicios de Internet informarán a los usuarios de sus derechos.**

7.2.4. Derecho a la educación digital.

El **sistema educativo garantizará la plena inserción del alumnado en la sociedad digital** y el aprendizaje de un consumo responsable y un uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales.

Las **Administraciones educativas deberán incluir en el desarrollo del currículo** la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada **utilización de las TIC**, con especial atención a las situaciones de violencia en la red.

El **profesorado recibirá las competencias digitales** y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.

Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.

Las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos.

7.2.5. Protección de los menores en Internet.

Los **padres, madres, tutores, curadores o representantes legales** procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales **determinará la intervención del Ministerio Fiscal**, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

7.2.6. Derecho de rectificación en Internet.

Todos tienen derecho a la libertad de expresión en Internet.

Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para **posibilitar el ejercicio del derecho de rectificación** ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.

Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Dicho aviso deberá aparecer en lugar visible junto con la información original.

7.2.7. Derecho a la actualización de informaciones en medios de comunicación digitales.

Toda **persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible** junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.

En particular, procederá la inclusión de dicho aviso cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. En este caso, el aviso hará referencia a la decisión posterior.

7.2.8. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.

Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

El **empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores** a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

Los empleadores deberán establecer **criterios de utilización** de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

7.2.9. Derecho a la desconexión digital en el ámbito laboral.

Los trabajadores y los empleados públicos tendrán **derecho a la desconexión digital** a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y

familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

El empleador, **previa audiencia de los representantes de los trabajadores**, **elaborará una política interna** dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

7.2.10. Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

Los empleadores **podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas**, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.

En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley.

7.2.11. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.

Los empleadores **podrán tratar los datos obtenidos a través de sistemas de geolocalización** para el ejercicio de las **funciones de control de los trabajadores o los empleados públicos** previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

7.2.12. Derechos digitales en la negociación colectiva.

Los convenios colectivos podrán establecer **garantías adicionales** de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

7.2.13. Protección de datos de los menores en Internet.

Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la **protección del interés superior del menor** y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.

Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.

7.2.14. Derecho al olvido en búsquedas de Internet.

Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona **cuando fuesen inadecuados,**

inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

El ejercicio del derecho al que se refiere este artículo no **impedirá el acceso a la información publicada en el sitio web** a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

7.2.15. Derecho al olvido en servicios de redes sociales y servicios equivalentes.

Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder **sin dilación** a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.

7.2.16. Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.

Los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible.

Los prestadores podrán conservar, sin difundirla a través de Internet, **copia de los contenidos cuando dicha conservación sea necesaria para el cumplimiento de una obligación legal.**

7.2.17. Derecho al testamento digital.

El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:

a) Las **personas vinculadas al fallecido por razones familiares o de hecho**, así como sus **herederos** podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión. Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.
b) El **albacea testamentario** así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.
c) En caso **de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal**, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

d) En caso de **fallecimiento de personas con discapacidad**, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones.

El responsable del servicio al que se le comunique, con arreglo al párrafo anterior, la solicitud de eliminación del perfil, deberá proceder sin dilación a la misma.

Mediante **real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones** y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta ley orgánica.

Lo establecido en este artículo en relación con las personas fallecidas en las comunidades autónomas con derecho civil, foral o especial, propio se regirá por lo establecido por estas dentro de su ámbito de aplicación.

7.2.18. Políticas de impulso de los derechos digitales.

El Gobierno, en colaboración con las comunidades autónomas, elaborará un Plan de Acceso a Internet con los siguientes objetivos:

a) **superar las brechas digitales** y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos mediante, entre otras medidas, un bono social de acceso a Internet;
b) **impulsar la existencia de espacios de conexión de acceso público**; y
c) **fomentar medidas educativas** que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales.

Asimismo se aprobará un **Plan de Actuación dirigido a promover las acciones de formación**, **difusión y concienciación** necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de

la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales.

El Gobierno **presentará un informe anual ante la comisión parlamentaria** correspondiente del Congreso de los Diputados en el que se dará cuenta de la evolución de los derechos, garantías y mandatos contemplados en el presente Título y de las medidas necesarias para promover su impulso y efectividad.