

Protección de datos personales

Miquel Colobran
Anna Chulià



Universitat Oberta
de Catalunya

Provisional

Índice

Introducción	7
Objetivos.....	8
1. La protección de datos.....	9
1.1. Que son los datos personales y datos sensibles	10
1.2. La normativa de protección de datos	12
1.3. Organizaciones sujetas al nuevo reglamento.....	13
2. Conceptos y definiciones.....	15
2.1. Ámbito de aplicación del RGPD y exclusiones	15
2.2. Ámbito de aplicación territorial.....	16
2.3. Definiciones.....	16
3. Principios generales	20
3.1. Relativos al tratamiento de los datos personales	20
3.2. Relativos a la protección de los datos personales	25
4. Legitimación del tratamiento	28
4.1. Consentimiento: otorgamiento y revocación.....	29
4.2. Consentimiento de los niños	30
4.3. Categorías especiales de datos	31
4.4. Bases jurídicas distintas al consentimiento	32
5. Derechos de las personas. Reglas generales aplicables.....	35
5.1. Ejercicio de los derechos.....	35
5.1.1. Acceso, rectificación, supresión (olvido).....	36
5.1.2. Derecho a la limitación de tratamiento	40
5.1.3. Derecho a la portabilidad.....	41
5.1.4. Derecho a no ser objeto de decisiones individuales	41
5.1.5. Limitaciones a los derechos	42
5.2. Derechos digitales de los ciudadanos en internet.....	43
5.3. Derechos relacionados con los menores.....	44
5.4. Derechos relacionados con el ámbito laboral.....	45
5.5. Derechos relacionados con medios de comunicación.....	47
5.6. Derecho al olvido en Internet.....	48
5.7. Derecho a la portabilidad	49
6. Responsabilidad proactiva	50
7. Figuras	52

7.1. Responsable de tratamiento (RT)	53
7.1.1. Funciones, obligaciones y responsabilidades	54
7.1.2. Tratamiento que no requiere identificación	55
7.2. Encargado de tratamiento (ET)	56
7.2.1. Funciones, obligaciones y responsabilidades	56
7.3. Delegado de protección de datos (DPD)	57
7.3.1. Funciones, obligaciones y responsabilidades	59
7.3.2. Obligatoriedad de la figura del DPD	60
7.3.3. Organizaciones que deben tener DPD	60
8. Medidas técnicas y organizativas	63
8.1. Análisis de riesgos	63
8.2. Registro de actividades de tratamiento (RAT)	64
8.3. Privacidad desde el diseño y por defecto	65
8.4. Evaluación de impacto	66
8.5. Medidas de seguridad	67
8.6. Notificación de violaciones de seguridad de los datos	68
9. Códigos de conducta y certificaciones	71
9.1. Códigos de conducta	71
9.2. Certificaciones	73
10. Transferencias internacionales	74
10.1. El sistema de decisiones de adecuación	74
10.2. Privacy shield	75
10.3. Normas corporativas vinculantes	75
10.4. Excepciones	75
11. Las autoridades de control y el régimen sancionador	77
11.1. Las autoridades de control	77
11.2. El régimen sancionador	78
Resumen	79
Glosario	81

Introducción

El objetivo principal de este módulo se cifra en facilitar los conocimientos necesarios para que un profesional conozca las obligaciones y, por tanto, las responsabilidades, en relación con la protección de datos bajo un prisma jurídico. Se pretende, por lo tanto, proporcionar los instrumentos teóricos y legislativos indispensables para que sepa identificar las conductas que pueden ser constitutivas de infracciones administrativas en materia de protección de datos así como la normativa que regula la conducta en las organizaciones y que afecta a todos los niveles.

Ante el nuevo escenario legislativo, es muy probable que a un profesional se le planteen numerosos interrogantes en el desempeño de su trabajo. Por ejemplo:

- ¿Contiene el buzón de mensajes datos personales de un trabajador?
- El servidor almacena datos de carácter personal y, por tanto, he de adoptar la implementación de medidas de seguridad determinadas. ¿Cuáles son?
- Si se produce un acceso no autorizado o una brecha de seguridad de los datos, ¿qué tengo que hacer? ¿Debo notificarlo a alguien?
- ¿Cuáles son los bienes jurídicos y derechos relacionados con la protección de datos personales

En este módulo intentaremos exponer las cuestiones esenciales que permitan solventar el mayor número posible de los interrogantes que se suscitan.

En primer lugar, haremos un recorrido sobre lo que representa la protección de datos, así como la motivación que lleva al derecho a regularla. Seguiremos con los conceptos fundamentales y derechos de la nueva ley. La nueva ley incorpora nuevas figuras para gestionar los datos, así como nuevos organismos. Terminaremos con una revisión sobre la vulneración de datos así como las sanciones relativas.

Objetivos

Los materiales didácticos de este módulo proporcionan los contenidos y herramientas imprescindibles para alcanzar los siguientes objetivos:

- 1.** Identificar las diferentes figuras que la nueva ley establece en la protección de datos.
- 2.** Identificar los datos sensibles y conocer cómo gestionarlos. En especial en relación con el propietario de los mismos (la persona).
- 3.** Identificar los organismos vinculados a la protección y cómo y en qué circunstancias hay que interactuar con ellos.
- 4.** Identificar situaciones de vulneración de datos y conocer cómo abordar la problemática.
- 5.** Conocer otros aspectos relativos a la nueva ley como la transferencia de datos internacionales fuera del espacio europeo.

1. La protección de datos

Es evidente que la información es apreciada por muchos aspectos relevantes. Por ejemplo, en el ámbito organizacional su importancia radica en la utilidad para la toma de decisiones o por su calidad de secreto industrial, por lo que en muchos casos es considerada el activo más importante. En otros casos, la información es fundamental para las operaciones de todos los días, aunque no siempre es propiedad de las empresas, sobre todo si consideramos que estos datos pueden pertenecer a los clientes o usuarios. Debido a la importancia de los datos y a los beneficios que pueden generar a los cibercriminales que buscan adueñarse de ellos, continuamente observamos brechas de seguridad relacionadas con la fuga de información, en los cuales se utilizan un conjunto cada vez más amplio y complejo de ataques para lograr los fines maliciosos. Además, el gran aumento del uso de Internet en la actualidad hace necesario una protección y una regulación que proteja los datos de las personas frente a usos no deseados. Es por todo ello que en los últimos años ha cobrado especial relevancia la protección de datos personales.


La protección de datos personales se ubica dentro del campo de estudio del Derecho Informático. Se trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no, es decir, no sólo a aquella información albergada en sistemas computacionales, sino en cualquier soporte que permita su utilización, almacenamiento, organización y acceso. En algunos países la protección de datos encuentra reconocimiento constitucional, como derecho humano y en otros es simplemente legal.

La diversidad de información que puede ser asociada a una persona es amplia. Los datos considerados como personales son utilizados para muchas actividades cotidianas. Pero la información puede encontrarse en distintas formas y con el avance tecnológico, muchos datos relacionados con los individuos se almacenan, procesan o transmiten en formato digital.

Esto expande el abanico de opciones para los cibercriminales que buscan lucrarse con la información, ya que ahora se utilizan los medios tecnológicos para cometer delitos, y es en este punto donde la seguridad de la información es muy importante, sobre todo porque cada brecha de seguridad relacionada con una fuga de información conlleva distintas consecuencias. Éstas están en función de los datos que son robados, el tipo de empresa que ha sido afectada, así como la industria o sector a la que pertenece dicha organización.

Dado que Internet se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva, “corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Inter-

net promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital”. En diversos países de nuestro entorno ya se ha aprobado normativa que además refuerza los derechos digitales de la ciudadanía.

La protección de datos trata la garantía o la facultad de control de la propia información frente a su tratamiento automatizado. 

Así pues, el derecho fundamental que la protección de datos persigue garantizar y proteger es el tratamiento de los datos personales y los derechos fundamentales de las personas físicas; especialmente, el derecho al honor e intimidad personal y familiar.

1.1. Que són los datos personales y datos sensibles

Se considera datos personales cualquier información relacionada con una persona física que se pueda utilizar para identificarla directa o indirectamente. Puede ser cualquier cosa: imagen, voz, información biométrica, una dirección IP, un nombre, una foto, una dirección de correo electrónico, datos bancarios, publicaciones en sitios web de redes sociales, información médica, nombre y apellidos, domicilio, dirección de correo electrónico, DNI, datos de geolocalización, etc.

Estos datos nos caracterizan como individuos y determinan nuestras actividades, tanto públicas como privadas. Debido a que cada dato está relacionado directamente con las personas, cada quien es dueño de sus datos personales y es quien decide si los comparte o no.

Entre estos datos se encuentran los que identifican a la persona, o aquellos que permiten tener comunicación con su titular. También, datos relacionados con el empleo, sobre características físicas como la fisonomía, anatomía o rasgos de la persona. Además, considera información relacionada con la formación y actividades profesionales, datos relativos a sus bienes, así como información biométrica.

Debido a que los datos personales pertenecen a su titular y no a las entidades que utilizan las bases de datos, se han puesto en marcha iniciativas alrededor del mundo, que buscan proteger los datos personales que se encuentran en posesión de particulares o de gobiernos, haciendo de la tarea de protección de la información, una responsabilidad compartida entre los usuarios, las empresas que tienen acceso a los datos y gobiernos que deben legislar al respecto, así como crear las instituciones encargadas de regular y hacer cumplir las leyes.

DATOS	
Identificación	Nombre, apellidos, estado civil, fotografía, edad, firma, fecha nacimiento, ...
Contacto	Domicilio, correo electrónico, teléfono....
Características físicas	Estatura, peso, complexión, color de piel, de iris o de cabello, tipo de sangre....
Patrimoniales	Bienes muebles, ingresos, cuentas bancarias, créditos,...
Laborales	Empresa, cargo, salario, domicilio y teléfono del trabajo,
Biométricos	Huella dactilar, patrón de retina, patrón de voz, forma de la mano,...
Académicos	Títulos, certificados, reconocimientos, formación no reglada,

Clasificación de datos personales

La UE (Unión Europea) ha ampliado sustancialmente la definición de datos personales.

La UE (Unión Europea) ha ampliado sustancialmente la definición de datos personales y los identificadores online, como las direcciones IP que ahora son considerados como datos personales. Otros datos, como la información económica, cultural o de salud mental, también se consideran información de identificación personal. Incluso, los datos personales pseudónimos también pueden estar sujetos a las reglas de la nueva ley, dependiendo de lo fácil o difícil que sea identificar cuáles son los datos.

⚠ Datos personales: toda información sobre una persona física identificada o identificable («el interesado»). Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona; La protección de datos trata la garantía o la facultad de control de la propia información frente a su tratamiento automatizado.

Artículo 4.1 del RGPD, y en los considerandos 26, 28 a 30, 34 y 35.

RGDP es el nuevo reglamento europeo de protección de datos. En los próximos apartados lo veremos con detalle.

No todos los datos de carácter personal son iguales ante la normativa. Hay determinados datos que por su relevancia y por su importancia para la privacidad deben tratarse y almacenarse con un mayor cuidado y cumpliendo una serie de requisitos. Estos datos son llamados datos sensibles o especialmente protegidos. Son una categoría de datos que debido a su incidencia especial en la intimidad, las libertades públicas y los derechos fundamentales de la persona, es necesaria una mayor protección que el resto de datos personales.

Algunos datos personales pueden resultar sensibles. En esta categoría se incluyen aquéllos que involucran el ámbito privado de su titular, cuyo uso indebido podría derivar en alguna afectación negativa, como la discriminación, por citar un ejemplo. Incluyen aspectos como el origen étnico, estado de salud, creencias religiosas, preferencia sexual, afiliación u opiniones políticas. Una posible clasificación por categorías puede verse en la figura.

DATOS	
Salud	Información genética, valoraciones médicas, informes médicos, ...
Vida sexual	Preferencias, hábitos sexuales, comportamiento...
Ideologías	Posicionamientos ideológicos, religiosos, filosóficos o morales. Ideas apolíticas o de afiliación sindical....
Origen étnico	Pertenencia a una etnia, identidades sociales, culturales y económicas, tradiciones o creencias....

Categorías de datos sensibles

Datos sensibles en la LOPD

Con el RGPD, se mantienen los datos que la antigua LOPD definía como especialmente protegidos los datos de ideología, religión, creencias, origen racial, salud, vida sexual, comisión o infracciones penales o administrativas) y añade tres categorías más:

datos genéticos,
datos biométricos,
orientación sexual.

1.2. La normativa de protección de datos

La existencia de tantos datos que pueden identificar o llegar a identificar una persona, lógicamente, provoca que el derecho tenga que regular el control de los datos personales, su tratamiento, medidas para protegerlas, así como las medidas para actuar en caso de vulneración. Las diferentes legislaciones sobre la protección de datos comienzan en el año 95 y en diciembre de 2018 se ha hecho la última adecuación y por tanto será la que vamos a ver en estos materiales.

Sólo como información de interés, las diferentes normativas que han existido han sido las siguientes:

- 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.
- Ley Orgánica 5/1992 de 29 de Octubre de Regulación del Tratamiento Automatizado de Datos de Carácter personal (LORTAD).

- Reglamento 994/1999 de 11 de junio, de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (reglamento LORTAD).
- La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El RGPD es el marco común de la comunidad europea en lo que respecta a la defensa de los datos personales. Antes, cada país tenía su propia regulación en esta materia, algo que no tenía demasiado sentido. Este reglamento europeo de protección de datos define derechos y obligaciones comunes a todos los estados miembros y a todos los ciudadanos europeos.

Los términos reglamento, GDPR, DRGP, Reglamento (UE) 2016/679 del Parlamento Europeo o nuevo reglamento de protección de datos hacen referencia a lo mismo, el texto del reglamento puede consultarse en:
<https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES>

La legislación vigente en materia de protección de datos es la ley 3/2018 de Protección de datos personales junto con el reglamento (UE) 2016/679 DEL PARLAMENTO EUROPEO. ⚡

La LOPDGDD lo que hace es completar exclusivamente el RGPD en aquellos aspectos en los que hace a remisiones.

Así pues en estos materiales haremos mención explícita tanto a la ley 3/2018 refiriéndonos a ella como “Ley” y al reglamento como “reglamento”, GDPR o RGDP a fin de intentar no confundiros.

1.3. Organizaciones sujetas al nuevo reglamento.

Todas las organizaciones están sujetas al nuevo reglamento si:

- La organización trata datos personales como parte de las actividades de una de sus sucursales establecidas en la Unión Europea (UE), independientemente del lugar donde sean tratados los datos, o

- La organización está establecida fuera de la UE y ofrece productos o servicios (de pago o gratuitos) u observa el comportamiento de las personas en la UE.

Si una organización es una pyme que trata datos personales según lo descrito arriba debe cumplir el Reglamento. Sin embargo, si el tratamiento de datos personales no constituye la parte principal de su negocio y su actividad no entraña riesgos para las personas, no estará sujeto a algunas obligaciones del RGPD, como por ejemplo el nombramiento de un delegado de protección de datos (DPD).

Cabe señalar que las «actividades principales» deben incluir actividades en las que el tratamiento de datos forme una parte indisoluble de la actividad del responsable o encargado del tratamiento

Ejemplo de cuando se aplica el reglamento.

En el caso de una empresa pequeña de enseñanza superior que opera por internet y está establecida fuera de la UE. Su actividad va destinada principalmente a universidades de lengua española y portuguesa de la UE. Ofrece asesoramiento gratuito en varios cursos universitarios y los estudiantes necesitan un nombre de usuario y una contraseña para acceder al material disponible en línea. La empresa ofrece dicho nombre de usuario y contraseña una vez los estudiantes han cumplimentado un formulario de matrícula.

Ejemplo de cuando no se aplica el reglamento.

En el caso de un proveedor de servicios de fuera de la UE que presta servicios a clientes de fuera de la Unión. Sus clientes pueden utilizar sus servicios cuando viajan a otros países, incluida la UE. Siempre que no dirija sus servicios específicamente a personas de la UE no estará sujeto a las normas del RGPD.

Están obligadas al cumplimiento las organizaciones, empresas, entidades y autónomos que hagan uso de los datos personales a nivel comercial dentro de la Unión Europea y también fuera, siempre y cuando ofrezcan servicios a consumidores o usuarios que estén dentro de la UE. !

2. Conceptos y definiciones

La nueva ley supone un cambio de enfoque respecto a la normativa anterior, la ley 15/1999 de protección de los datos personales (LOPD), pues establece una lógica basada en la responsabilidad y en la transparencia, mientras que la LOPD se basaba en gran parte en mecanismos formales como la declaración y la autorización.

Algun término que aparece ahora se define dentro del reglamento. Consultad el glosario en caso de duda.

Toda persona tiene derecho a la protección de sus datos personales. En base a ello, es importante saber que no deberíamos tratar datos de terceros si no conocemos esos derechos. !

2.1. Ámbito de aplicación del RGPD y exclusiones

El art. 2 del RGPD establece el ámbito de aplicación material del Reglamento, así como sus exclusiones. El RGPD se aplicará a todo tratamiento de datos personales, sea por medios automatizados o no automatizado, contenidos o destinados a ser incluidos en un fichero (art.2.1).

El RGPD se aplica a las personas físicas en relación al tratamiento de sus datos personales. No es de aplicación al tratamiento de datos personales relativos a las personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.

No entran en el ámbito de aplicación del RGPD los ficheros o conjuntos de ficheros que no estén estructurados con arreglo a criterios específicos. En el apartado 2º del artículo 2 del RGPD se establecen determinados supuestos en los que se excluye la aplicación del mismo. Dichas exclusiones son las siguientes:

- a) cuando se trate de una actividad no comprendida en el ámbito del derecho de la Unión (UE); Se refiere a cuestiones relativas a la protección de los derechos y las libertades fundamentales o a la libre circulación de datos personales relacionadas con la seguridad nacional.
- b) los realizados por los Estados Miembros (en adelante EM) cuando lleven a cabo actividades relacionadas con la política exterior y de seguridad común de la UE.

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

Se entenderá por actividades exclusivamente personales o domésticas aquellas que no tengan ninguna conexión con una actividad profesional o comercial. El RGPD menciona a modo de ejemplos la correspondencia y las agendas personales, o la actividad en las redes sociales siempre que no sean utilizadas con finalidades comerciales o profesionales. Sin embargo, el RGPD sí será de aplicación a los responsables o encargados de tratamiento que proporcionen los medios para tratar datos personales relacionados con las actividades personales o domésticas, por ejemplo, a las redes sociales como FaceBook, Twitter, etc.

d) los efectuados por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención.

e) Los tratamientos de datos personales efectuados por las autoridades competentes para dichos fines se regirán por la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo.

f) El RGPD tampoco se aplica a la protección de datos personales de las personas fallecidas. Si bien, deja en manos de los EM la competencia para establecer las normas relativas al tratamiento de los datos personales de estas.

2.2. Ámbito de aplicación territorial.

El RGPD se aplica al tratamiento de datos personales en el contexto de un establecimiento del responsable o del encargado de tratamiento (en adelante RT o ET) en la Unión Europea (UE), independientemente de que el tratamiento tenga lugar en la UE o fuera de ella. Un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables, independientemente de la forma jurídica que se haya adoptado, sea una sucursal o una filial con personalidad jurídica.

En el apartado de **Figuras** veremos con detalle la figura del encargado de tratamiento y responsable de tratamiento

2.3. Definiciones

En muchas ocasiones el lenguaje común no se corresponde con la definición de los términos legales, y en otras necesita ser precisado. Teniendo en cuenta lo anterior el art. 4 del RGPD proporciona una serie de definiciones de algunos de los términos más importantes utilizados en el RGPD.

a) Datos personales.

Toda información sobre una persona física identificada o identificable («el interesado»). Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona

b) Datos sensibles. Categorías especiales de datos.

Categorías especiales de datos (datos personales sensibles): datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, los 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 orientaciones sexuales (artículo 9 de la Ley).

Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de esa persona.

Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Datos relativos a la salud: datos relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud. Entre otros: la información recogida en la inscripción a efectos de la prestación de asistencia sanitaria, la recogida con prestación de tal asistencia; todo número, símbolo o dato asignado a una persona que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes, incluida la procedente de datos genéticos y muestras biológicas; y cualquier información relativa a una enfermedad, discapacidad, riesgo de padecer enfermedades; el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente.

El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales. Únicamente se considerarán datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.

c) Tratamiento y Limitación del Tratamiento.

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos

automatizados o no, como la recogida, registro, organización estructuración o conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación supresión o destrucción.

Limitación del tratamiento: El derecho a la limitación del tratamiento permite al interesado, cuyos datos personales son objeto de tratamiento, solicitar al responsable del tratamiento que aplique medidas sobre esos datos para, entre otras cosas, evitar su modificación o su borrado o supresión (artículo 16 de la Ley).

Fichero vs tratamiento.

Al fichero “clientes” se le pueden atribuir diferentes tratamientos, como:

La prestación de un servicio o venta de un producto.

Envío de publicidad de otros productos o servicios de la organización.

Envío de información sobre eventos organizados por la empresa.

d) Anonimización o Disociación

Es el proceso por el cual los datos se eliminan de manera irreversible. Con la anonimización, el dato personal se disociará por completo, por lo que un sujeto no podrá ser identificado. Desde ese momento, su tratamiento no entraría dentro del ámbito del Reglamento General de Protección de Datos.

Como consecuencia, el responsable del tratamiento podrá hacer uso de esa información ya que no afecta a la privacidad del individuo. Al ser imposible conocer su identidad, esa información pasa a ser un dato empresarial en lugar de personal. Sin embargo, el uso de la anonimización es muy limitado y hay que saber muy bien cómo realizarlo y cuándo se puede llevar a cabo.

e) Seudonimización

El tratamiento de datos personales de manera que ya no puedan atribuirse al interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

“aquella información que, sin incluir los datos denominativos de un sujeto, permiten identificarlo mediante información adicional, siempre que ésta figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.” (artículo 4.5 del RGPD). Laseudonimización solo reemplaza parte del conjunto de datos y no permite la identificación directa del sujeto. Sin embargo, se puede averiguar la identidad del sujeto a través de informaciones adicionales. Por tanto, laseudonimización está sujeta al RGPD.

La Agencia Española de Protección de Datos (AEPD) señala en su guía ‘Orientaciones y garantías en los procedimientos de anonimización de datos personales’ que “el artículo 9 del RGPD recomienda la existencia de un equipo para el estudio de la viabilidad del proceso de anonimización, especialmente si se trata de datos protegidos”.

Además, “el personal implicado debe conocer y cumplir todos los aspectos relacionados con la nueva normativa de protección de datos.”

Según el Dictamen 05/14 del Grupo de Trabajo sobre Protección de Datos de Carácter del artículo 29, las técnicas deseudonimización más frecuentes son: el cifrado con clave secreta, la función hash, la función con clave almacenada, el cifrado determinista o función hash con clave de borrado de clave y la descomposición en tokens.

Ejemplo.

Se puede cambiar el nombre, la dirección o la fecha de nacimiento de un sujeto, pero no todos sus datos estarán “enmascarados”. Con informaciones complementarias se puede llegar a identificar a ese sujeto, lo que nos sitúa dentro del ámbito de los datos personales y, por consiguiente, del Reglamento europeo.

f) Fichero

Conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Por ejemplo, “ficheros de recursos humanos”, “fichero de clientes”, etc. El RGPD y la nueva Ley suprimen esta expresión y la reemplazan por la palabra “tratamiento”. Ya no se habla de “ficheros de datos personales”, sino de “tratamientos de datos personales”.

g) Responsable y Encargado de tratamiento.


Responsable del tratamiento: persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

Encargado de tratamiento: persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos por cuenta del responsable del tratamiento.

Más adelante veremos con detalle la figura del encargado de tratamiento y responsable de tratamiento dir apartat ¡!

g) Destinatario.

Persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen los datos, se trate o no de un tercero. No obstante, no se consideraran destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de acuerdo con el Derecho de la UE o de los EM.

Para otros conceptos y definiciones relevantes consultar el art. 4 del reglamento. 

3. Principios generales

3.1 Relativos al tratamiento de los datos personales

Estos 6 principios que prevé el nuevo RGPD son, de hecho, una versión mejorada de los ya regulados en la LOPD. Y por supuesto se convierten en obligaciones para el Responsable del Tratamiento. Podríamos decir que el más significativo de los principios es el de transparencia.

Cuanto más transparente sea el Responsable del Tratamiento, con el titular de los datos, mejor se estará implementando la nueva normativa y más control tendrá este sobre sus datos personales. Hacer un buen uso de los datos personales es muy importante, ya no por el hecho de cumplir con las normas impuestas, sino para respetar los derechos de los usuarios y su intimidad.

A los tradicionales principios de calidad: **proporcionalidad, finalidad, exactitud y actualidad, cancelación de oficio y licitud**, el RGPD incorpora través del art. 5, seis principios básicos.

El RGPD establece la transparencia como principio clave, puesto que es el camino hacia la excelencia en la protección de los derechos de los interesados.

a) Principio de Minimización de Datos

Lo que pretende es limitar el uso de datos estrictamente a aquellos datos que sean considerados como adecuados, pertinentes y limitados en relación con las finalidades para las cuales sean tratadas (art. 5.1.c RGPD).

Sería equiparable o quedar incluido con la antigua LOPD. En lo que conocíamos como el Principio de Proporcionalidad.

El principio de minimización de datos implica que solo se tratarán datos personales cuando la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. En tal caso únicamente se tratarán los datos personales adecuados y necesarios para lograr los fines establecidos en el momento de su recogida (art. 5.1 d) RGPD).

b) Principio de Limitación de la Finalidad

Pretende que los objetivos perseguidos sean determinados, explícitos y legítimos. Está reflejado en el artículo 5.1.b. “Los datos personales 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 (art. 5.1.b)”. No estamos hablando ya de finalidades distintas, sino de finalidades incompatibles.

Anteriormente era conocido como el Principio de Finalidad.

El principio de limitación de la finalidad del tratamiento supone que los datos deberán ser recogidos para fines determinados, explícitos y legítimos y

deben determinarse en el momento de la recogida. También exige que no sean tratados ulteriormente de manera incompatible con dichos fines (art.5.1 b) RGPD).

Por lo tanto, el tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo se permite cuando el tratamiento sea compatible con los fines para los que se han recogido inicialmente. Conforme al RGPD se consideran fines compatibles el tratamiento ulterior de los datos personales que sea necesario para el cumplimiento de una misión en interés público conferida al RT, siempre que se encuentren determinados por el Derecho de la UE o de los EM.

Por mandato legal no se consideraran incompatibles el tratamiento ulterior de datos con los fines siguientes (art. 89.1 RGPD):

- a) archivo en interés público;
- b) investigación científica e histórica;
- c) estadísticos;

En todo caso, para determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el RT tendrá en cuenta, entre otros:

- a) la relación existente entre los fines de la recogida inicial y los fines del tratamiento ulterior
- b) el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado en cuanto a su uso posterior;
- c) la naturaleza de los datos personales, en particular si se trata de datos sensibles o datos relativos a condenas o infracciones penales;
- d) las posibles consecuencias para los interesados del tratamiento ulterior previsto, y
- e) la existencia de garantías adecuadas en la operación de tratamiento original y ulterior como, por ejemplo, el cifrado y la seudonimización de los datos.

Si el interesado dio su consentimiento al tratamiento o el tratamiento se basa en el Derecho de la UE o de los EM y constituye una medida necesaria y proporcionada para salvaguardar el interés público general, el responsable está facultado para realizar el tratamiento ulterior, con independencia de la compatibilidad de los fines. Con todo, deberá garantizar la aplicación de los principios del RGPD, en particular la información del interesado sobre esos

otros fines y los derechos que le asisten, incluido el derecho de oponerse al tratamiento.

c) Principio de Exactitud de los Datos

El artículo 5.1.d establece que los datos personales deben ser “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 (art. 5.1.d RGPD)”. El nuevo reglamento insiste en que los datos sean exactos y actualizados. Por lo tanto, el responsable del tratamiento deberá actuar con la diligencia necesaria para hacer un buen uso de los datos. Es decir, que sean correctos, completos y actuales.

Este nuevo principio coincide en cierta manera con el conocido anteriormente como Principio de Calidad de los Datos

Para ello el RT adoptará medidas razonables para suprimir o rectificar sin dilación los datos inexactos (art. 5.1 d) RGPD).

d) Principio de Limitación del Plazo de Conservación

Dicho principio tiene por objetivo limitar temporalmente el uso de datos personales. Así pues, obliga a cesar en su tratamiento cuando estos dejan de ser necesarios para la finalidad perseguida. Concretamente se encuentra regulado en los siguientes términos: “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. Añade que “los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público. También, “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 (artículo 5.1.e RGPD).

Los datos personales no se podrán conservar más allá del tiempo necesario para cumplir con los fines del tratamiento (art. 5.1 e) RGPD).

Si bien, el RGPD establece algunas excepciones a la limitación del plazo de conservación, siempre que:

- a) se traten exclusivamente con fines de investigación científica o histórica o fines estadísticos, y
- b) se apliquen las medidas técnicas y organizativas apropiadas para proteger los derechos y libertades de los interesados.

Para garantizar que los datos personales no se conservan más tiempo del necesario, el RT deberá establecer plazos para su supresión o revisión periódica.

e) Principio de Seguridad

El objetivo de este principio es garantizar una seguridad adecuada, integridad y confidencialidad de los datos personales. Se encuentra regulado en el artículo 5.1.f en los términos siguientes: “los datos personales serán 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 (art. 5.1.f RGPD)”. Lo que pretende el RGPD es proteger los derechos de los interesados. Por ello, a pesar de seguir existiendo el principio de seguridad, cuando implementemos las medidas concretas deberemos evaluar los riesgos que suponen el tratamiento de dichos datos para los derechos de los interesados. Se deberá realizar un análisis de riesgo que establezca las medidas de seguridad adecuadas al riesgo, aplicarlas y supervisarlas periódicamente, aplicando técnicas de cifrado de datos, controles de acceso, copias de respaldo, antivirus, etc. Todo lo necesario para garantizar la integridad, la disponibilidad y la confidencialidad de esos datos que afectan a personas.

Ya anteriormente se aplicaban medidas de seguridad técnica y organizativa para proteger los datos personales.

Se garantizará la seguridad de los datos personales, incluido el tratamiento no autorizado o ilícito de los mismos, así como contra su pérdida, destrucción o daño accidental mediante medidas de seguridad técnicas y organizativas (art. 5.2 f) RGPD).

Además, con el fin de garantizar la integridad y confidencialidad de los datos, el RGPD establece una serie de obligaciones que el RT deberá cumplir. Por ejemplo:

- Evaluación de riesgos
- Notificación de violaciones de seguridad.

f) Principio de licitud, lealtad y transparencia

Regulado en el artículo 5.1.a, dicho principio pretende exigir que el responsable cumpla con la obligación de facilitar al interesado la información relativa al tratamiento de forma explícita. Además, también concisa, transparente, inteligible y de fácil acceso. En concreto, el artículo dice: “los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado (art. 5.1.a RGPD)”.

El RGPD pretende con este principio, dejar atrás los textos cargados de lenguaje jurídico dirigidos a personas no juristas. Si el usuario tiene que conocer qué pasa con sus datos, deberá disponer de una información inteligible.

Además se establece que a efectos de la Ley RGPD no serán imputables al responsable del tratamiento (siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación) la inexactitud de los datos obtenidos directamente del afectado cuando hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad, o cuando el responsable los obtuviese del mediador o intermediario cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador o cuando los datos hubiesen sido obtenidos de un registro público.

Todo tratamiento de datos personales debe ser además de lícito, leal y transparente. Para la persona ha de quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando sus datos personales.

El principio de lealtad y el de transparencia van íntimamente ligados y exigen que se informe al interesado de la existencia de la actividad de tratamiento y de sus fines. De acuerdo con el RGPD el principio de transparencia exige que toda la información y comunicación relativa al tratamiento de los datos personales sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. En particular deberá facilitarse a los interesados la información sobre la identidad del RT y los fines del tratamiento, y toda la información necesaria con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento.

También deberá facilitarse cuanta información complementaria sea necesaria para garantizar que el tratamiento sea leal y transparente, atendiendo a las circunstancias y al contexto específico del tratamiento. El RGPD exige que se informe al interesado la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración.

En situaciones de complejidad tecnológica o en las que proliferen diversos agentes puede ser conveniente que la información se facilite en forma electrónica mediante un sitio web, especialmente cuando dicha información se dirige al público en general. Este podría ser el caso de la publicidad en línea, pues al interesado le resulta difícil saber y comprender si se están recogiendo sus datos personales, por quién y con qué finalidad.

El RGPD contempla una nueva modalidad de facilitar información utilizando la información en combinación con iconos normalizados que ofrezcan de manera fácilmente visible, inteligible y legible una adecuada visión del conjunto del tratamiento previsto. Cuando se presenten iconos en formato electrónico estos deberán ser legibles mecánicamente.

En definitiva, las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardas y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento.

La transparencia de la información se configura en el RGPD como uno de los derechos de los interesados, lo cual implica que toda la información que el RT deba facilitar al interesado lo hará de manera transparente. Por ello la información que el RT deba facilitar al interesado deberá hacerlo en forma concisa, transparente, inteligible, de fácil acceso, utilizando un lenguaje claro y sencillo, especialmente cuando la información se dirige a un niño. Se deberán evitar las fórmulas farragosas con remisiones a textos legales. Dicha información podrá facilitarse por escrito o por otros medios. El RGPD contempla la posibilidad de que la información pueda facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

La información que deberá facilitarse a los interesados en la recogida de sus datos personales podrá realizarse mediante una combinación con iconos normalizados que permitan una visión de conjunto del tratamiento previsto.

Se incrementa la información que el RT deberá facilitar a los interesados en el momento de la recogida de los datos personales. En el siguiente cuadro aparece en la columna de la izquierda la información que se debía facilitar conforme a la LOPD y en el de la derecha la que se deberá facilitar conforme el RGPD.

Las Autoridades de Protección de Datos españolas en el documento conjunto que han elaborado "Guía para el cumplimiento del deber de informar" aconsejan adoptar un modelo de información por capas como la manera de conciliar los requerimientos de proporcionar mayor información con la exigencia de transparencia que impone el RGPD.

Para saber más se aconseja una lectura de la "Guía para el cumplimiento del deber de informar" de la AEPD que encontrareis aquí

<https://www.aepd.es/reglamento/cumplimiento/principio-responsabilidad-proactiva.html>

3.2 Relativos a la protección de los datos personales

Los principios generales de la protección de datos de carácter personal son un conjunto de reglas que determinan cómo recoger, tratar y ceder los datos. En definitiva, son deberes y obligaciones a los que están sujetos los tratamientos de datos de carácter personal.

En caso de encontrarnos con lagunas o vacíos legales, nos hemos de inspirar en éstos, para que el tratamiento de los datos sea conforme a la normativa.

Exactitud (art 4 Ley)

Los datos deben ser exactos y, si fuera necesario, actualizados. Deben adoptarse todas las medidas razonables para corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.

Deber de confidencialidad (art 5 Ley)

Debe garantizarse una seguridad adecuada para preservar la integridad de los datos e impedir el acceso o uso no autorizado. Todas las personas que intervengan en cualquier fase del tratamiento están sujetas a guardar secreto o confidencialidad con carácter indefinido.

Licitud o legitimación del tratamiento (art. 6 Ley)

Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento explícito del interesado o sobre otra base o fundamento jurídico.

En el siguiente apartado se trata con detalle este artículo.

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

Licitud o legitimación del tratamiento de menores de edad (art. 7 Ley)

Para que el tratamiento sea lícito únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. En los menores de catorce años, 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.

Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos (art 8. Ley)

Solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 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.

Categorías especiales de datos (art 9. Ley)

La Ley se remite al artículo 9.2.a) del Reglamento (UE) 2016/679.

Datos de naturaleza penal (art 10. Ley)

El tratamiento de datos personales relativos a condenas e infracciones penales sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesa-

La Ley se remite al artículo 10 del Reglamento

dos. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

4. Legitimación del tratamiento.

A partir de los principios vistos, que deben cumplirse, ahora pasamos a ver bajo que situaciones el tratamiento de datos se puede realizar. Es decir, cuando es lícito. Para que un tratamiento sea lícito los datos deberán ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida en el RGPD. El RGPD mantiene el principio recogido en la Directiva 95/46, transpuesto en el derecho español en la LOPD, según el cual todo tratamiento de datos debe apoyarse en una base jurídica que lo legitime. En este sentido el RGPD sigue manteniendo las bases jurídicas establecidas por la Directiva 95/46. Sin embargo, cabe señalar la introducción de novedades significativas en lo que respecta a los tratamientos apoyados en el consentimiento y en el interés legítimo.

Conforme el art. 6 de RGPD un tratamiento lícito deberá cumplir al menos una de las siguientes condiciones:

- a) el interesado ha dado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
- b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación de medidas precontractuales solicitadas por el interesado;
- c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
- d) el tratamiento es necesario para proteger los intereses vitales del interesado o de otra persona física.
- e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al RT.
- f) es necesario para la satisfacción de intereses legítimos perseguidos por el RT o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

La licitud o legitimidad en el tratamiento de datos se encuentra regulado en el art. 6 y en los considerandos 41, y 45 a 50 del reglamento.



Vamos a desarrollar algunos de los aspectos más significativos o que suponen novedades respecto a la legislación anterior.

4.1. Consentimiento: otorgamiento y revocación

El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de los datos personales que le conciernen.

El RT deberá ser capaz de demostrar que el interesado ha dado su consentimiento al tratamiento de sus datos personales. No se considerará que el consentimiento se ha prestado libremente en los siguientes supuestos, cuando:

- el interesado no goza de verdadera o libre elección;
- el interesado no pueda denegar o retirar su consentimiento sin sufrir perjuicio alguno;
- exista un desequilibrio claro entre interesado y RT, en particular cuando el RT sea una autoridad pública.
- no permita autorizar por separado las distintas operaciones de tratamiento pese a ser adecuado en el caso concreto;
- el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento.

El consentimiento inequívoco requiere que se preste mediante una manifestación del interesado o mediante una acción clara afirmativa. A diferencia de la legislación anterior el RGPD no contempla el consentimiento tácito o por omisión.

Existen situaciones en las que el consentimiento, además de inequívoco, deberá de ser explícito:

- cuando se categorías especiales de datos,
- en las transferencias internacionales de datos,
- cuando se adopten decisiones individuales automatizadas.

El consentimiento podrá otorgarse por escrito, inclusive por medios electrónicos, o mediante una declaración verbal. Cuando el consentimiento se da mediante declaración escrita que contenga otros asuntos, la solicitud de consentimiento se distinguirá claramente del resto de asuntos, deberá ser inteligible y se utilizará un lenguaje claro y sencillo.

Las formas de otorgar el consentimiento podrían incluir:

- marcar una casilla de un sitio web en internet,
- escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o
- cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta que sus datos personales sean tratados.

Por tanto, en ningún caso se entenderá otorgado el consentimiento cuando aparezcan las casillas premarcadas, el silencio o la inacción.

El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo fin o fines. Por tanto, cuando el tratamiento tenga varios fines deberá darse el consentimiento para todos ellos.

En cuanto a la revocación del consentimiento prestado, el interesado tendrá derecho a retirar su consentimiento en cualquier momento y deberá ser tan fácil retirarlo como darlo. Los efectos de la revocación surgirán a partir del momento de la retirada, sin que ello afecte a la licitud del tratamiento previo a la retirada.

¿Qué ocurre con los tratamientos iniciados antes de la aplicación del RGPD, cuya legitimidad se base en el consentimiento otorgado conforme a la Directiva 95/46/CE?

En este supuesto no será necesario que el interesado dé su consentimiento de nuevo si la forma en la que se otorgó el consentimiento se ajusta a las condiciones del RGPD. Por tanto, en aquellos casos en que la base del tratamiento sea el consentimiento tácito, se deberá solicitar el consentimiento conforme al RGPD.

4.2. Consentimiento de los niños.

El RGPD considera que se debe dar una protección específica a los datos personales de los menores, ya que los menores suelen ser menos conscientes de los riesgos, consecuencias, garantías y de los derechos que les asisten.

En el contexto de la oferta directa de servicios de la sociedad de la información a los niños, únicamente será válido el consentimiento del menor que tenga como mínimo 16 años. Además, la información facilitada al menor deberá realizarse en un lenguaje claro y sencillo y fácil de entender para el niño. Si el niño es menor de 16 años, se requerirá autorización de quien tenga la patria potestad o tutela del menor, sin la cual el tratamiento no sería lícito.

A pesar de que el RGPD establece el umbral de edad a partir del cual el menor puede consentir sin necesidad del titular de la patria potestad o tutela, este deja abierta la posibilidad para que los EM establezcan una edad inferior siempre que no sea inferior a 13 años.

**Son los comúnmente llamados
proxies o servidores proxy.**

El opt-in

Es un sistema que se exige una autorización por parte del interesado antes del envío de cualquier tipo de publicidad por correo electrónico.

Para saber más puedes consultar Guidelines on Consent under Regulation 2016/679 (wp259rev.01)

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

El RGPD obliga al RT a verificar que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño y le obliga a realizar esfuerzos razonables para ello, sobre la base de la tecnología disponible.

4.3. Categorías especiales de datos

El RGPD otorga una protección especial a aquellos datos que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, cuyo tratamiento podría suponer riesgos importantes para los derechos fundamentales.

Una de las novedades del RGPD respecto a la normativa anterior es la introducción de nuevas categorías especiales de datos. Ciertamente, a las contempladas anteriormente se añaden:

- los datos biométricos dirigidos a identificar de manera unívoca a una persona física,
- los datos genéticos.

En principio el RGPD prohíbe el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, los datos de salud o los relativos a la vida sexual o las orientaciones sexuales de una persona, además de los datos genéticos y biométricos (art. 9.1 RGPD).

Sin embargo, también establece excepciones a la prohibición general de tratamiento de esta categoría especial de datos. Son las siguientes:

- el interesado ha dado el consentimiento explícito para uno o más fines especificados;
- en el ámbito del Derecho laboral y de la seguridad social, cuando el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del RT o del trabajador. El tratamiento se podrá realizar en la medida en que así esté autorizado por el Derecho de la UE, de los EM o por un convenio colectivo ajustado a derecho. Además, se deberá garantizar el respeto a los derechos fundamentales y a los intereses del trabajador.
- cuando el tratamiento sea 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;
- cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales y el tratamiento se refiera exclusivamente a los miembros actuales o antiguos. Sin em-

Sobre los tratamientos en el ámbito laboral puede consultarse la Opinión del GT29 2/2017 on data processing at work.

bargo, los datos personales no podrán comunicarse a terceros sin consentimiento de los interesados;

- cuando el tratamiento se refiera a datos personales que el interesado haya hecho manifiestamente públicos;
- cuando el tratamiento sea necesario por razones de interés público, en particular en el ámbito de la salud pública y la gestión de los servicios de asistencia sanitaria; con fines de seguridad, supervisión y alerta sanitaria para la prevención o control de las enfermedades transmisibles y otras amenazas graves para la salud; en el ámbito de la legislación laboral y de protección social, incluidas las pensiones;
- de manera excepcional cuando el tratamiento sea necesario para el ejercicio de acciones judiciales o reclamaciones en procedimientos administrativos o extrajudiciales.
- con fines de archivo en interés público, de investigación científica e histórica o estadística.

El RGPD también contempla la posibilidad de que los EM puedan introducir condiciones adicionales, incluso limitaciones respecto al tratamiento de los datos genéticos, biométricos o los datos relativos a la salud.

4.4. Bases jurídicas distintas al consentimiento.

El RGPD mantiene las mismas bases jurídicas que legitiman los tratamientos de datos personales. Recordemos cuáles son:

- el consentimiento,
- la existencia de una relación contractual,
- la protección de los intereses vitales del interesado o de una tercera persona,
- una obligación legal para el RT,
- existencia de un interés público o el ejercicio de poderes públicos,
- los intereses legítimos prevalentes del RT o de terceros a los que se comunican los datos.

Una de las novedades que introduce el RGPD respecto a la legislación anterior es la obligación del RT de identificar y documentar la base jurídica que justifica cada tratamiento. Este extremo es indispensable para demostrar que se cumple con las disposiciones del RGPD. Algunos ejemplos:

- se obliga al RT a incluir la base jurídica que justifica el tratamiento en la información que se facilita al interesado en el momento de la recogida de los datos;
- especificar y documentar los intereses legítimos en que se fundamentan los tratamientos en las Evaluaciones de Impacto o en determinadas Transferencias internacionales de datos.

Conforme el art. 6 de RGPD un tratamiento lícito deberá cumplir al menos una de las siguientes condiciones:

- a) el interesado ha dado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
- b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación de medidas precontractuales solicitadas por el interesado;
- c) es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

Cuando el tratamiento se realice en cumplimiento de una obligación legal aplicable al RT, o cuando es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la UE o de los EM. No hace falta que cada tratamiento individual se rija por una norma específica, siendo suficiente una norma que sirva de base para varias operaciones de tratamiento basadas en una obligación legal o para el cumplimiento de una misión realizada en interés público.

- d) es necesario para proteger los intereses vitales del interesado o de otra persona física. Los datos personales únicamente deben tratarse sobre la base del interés vital del interesado cuando el tratamiento no pueda basarse en otra de las bases jurídicas establecidas en el RGPD.

Este tipo de tratamientos pueden responder tanto a motivos de interés público como a los intereses vitales del interesado. El RGPD cita ejemplos tales como los fines humanitarios, incluido el control de epidemias, o en situaciones de emergencia humanitaria producidas por catástrofes naturales o de origen humano.

- e) es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al RT. El RGPD menciona como ejemplo de misión realizada en interés público, siempre que se ofrezcan garantías adecuadas, la autorización del tratamiento de los datos personales realizados por los partidos políticos que recopilen datos personales sobre las opiniones políticas de las personas.

- f) es necesario para la satisfacción de intereses legítimos perseguidos por el RT o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

En este supuesto siempre deberá realizarse una evaluación y ponderación entre el interés legítimo perseguido por el RT o de un tercero y los derechos y libertades de los interesados, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el RT. Se deberá también evaluar si un interesado puede prever de forma razonable, en el momento y contexto de la recogida de sus datos personales, que pueda producirse el tratamiento con tal fin.

El RGPD cita algunos ejemplos de interés legítimo del RT:

- a) la prevención del fraude cuando el tratamiento de datos personales es estrictamente necesario;
- b) el tratamiento con fines de mercadotecnia directa;
- c) el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información.

Este punto se refiere a la capacidad de una red o sistema de información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de estos sistemas o redes por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de repuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. Un ejemplo de lo anterior sería impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, o frenar ataques de "denegación de servicio"; así como, evitar daños a los sistemas informáticos y de comunicaciones electrónicas. d) Interés legítimo podría ser la transmisión de datos personales dentro de un grupo empresarial para fines administrativos internos.

5. Derechos de las personas. Reglas generales aplicables

La nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales, además de destinarse a adaptar el ordenamiento español al Reglamento general de protección de datos y completar sus disposiciones, incorpora a su objeto la importante novedad de dirigirse a “garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución” (art. 1.b). Este contenido se ha concretado en el Título final de esa Ley, el décimo, titulado precisamente “Garantía de los derechos digitales”, compuesto de 19 artículos (del 79 al 97).

En el mismo se reconoce y regula el ejercicio de derechos como el de neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital, la libertad de expresión en internet, el derecho al olvido en buscadores y redes sociales, a la portabilidad, al testamento digital, a la intimidad en el uso de dispositivos digitales en el ámbito laboral y a la desconexión digital.

El RGPD contempla los conocidos como derechos ARCO recogidos en la legislación anterior y añade dos nuevos derechos: limitación del tratamiento y portabilidad. Además, establece la diferencia entre el derecho de rectificación y el derecho de supresión (derecho al olvido).

5.1. Ejercicio de los derechos

La normativa de protección de datos permite poder ejercer ante el responsable del tratamiento tus derechos de acceso, rectificación, oposición, supresión (“derecho al olvido”), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas.

Estos derechos se caracterizan por lo siguiente (art. 12 Ley):

- Su ejercicio es gratuito
- Si las solicitudes son manifiestamente infundadas o excesivas (p. ej., carácter repetitivo) el responsable podrá:
 - Cobrar un canon proporcional a los costes administrativos soportados
 - Negarse a actuar

- Las solicitudes deben responderse en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses más
- El responsable está obligado a informarte sobre los medios para ejercitar estos derechos. Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que se opte por otro medio
- Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo
- Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una Autoridad de Control
- Se pueden ejercer los derechos directamente o por medio de un representante legal o voluntario
- Cabe la posibilidad de que el encargado sea quien atienda la solicitud por cuenta del responsable si ambos lo han establecido en el contrato o acto jurídico que les vincule

5.1.1. Acceso, Rectificación, Supresión (olvido)

Derecho de acceso (art 13). Los interesados tienen derecho a acceder a los datos personales recogidos por el RT que le conciernan, a obtener del RT confirmación de si se están tratando o no sus datos personales y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento.

Por ejemplo.

Los interesados tienen derecho a acceder a los datos relativos a sus historias clínicas que contengan información sobre diagnósticos, evaluaciones de facultativos, resultados de pruebas o intervenciones practicadas.

El interesado tiene derecho a acceder a la siguiente información (art.15 RGPD):

- los fines del tratamiento;
- las categorías de datos personales tratados;
- los destinatarios a los que se comunican o se tenga previsto comunicar los datos y si se prevé realizar TID y las garantías que se aplicarán;
- el plazo previsto de conservación;
- posibilidad de ejercitar los derechos de rectificación, supresión, limitación del tratamiento u oposición al tratamiento, y posibilidad de reclamación ante la autoridad de control;
- existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos la lógica aplicada y las consecuencias previstas para el interesado.

En general, el modo de acceso será mediante copia de los datos personales objeto del tratamiento y tendrá carácter gratuito. Si bien, cuando el interesado solicite más de una copia, el RT podrá percibir un canon razonable por los costes administrativos. El RGPD también contempla que el RT pueda facilitar el acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales. Además, cuando la solicitud de acceso se realice por medios electrónicos la información se facilitará por dichos medios, a menos que el interesado solicite otro modo de acceso.

El derecho de acceso a los datos personales en ningún caso afectará negativamente los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual, en particular la propiedad intelectual que protege los sistemas informáticos. No obstante, en ningún caso puede negarse a ofrecer información al interesado.

Cuando el RT tenga una gran cantidad de información del interesado, el RT puede solicitar al interesado que especifique la información a la cual desea acceder.

El RT deberá utilizar las medidas razonables para verificar la identidad de los solicitantes, en particular cuando se presten servicios en línea.

El RT no deberá conservar datos personales con el único propósito de poder responder a las solicitudes.

Derecho de rectificación (art 14). El ejercicio de este derecho supone que el interesado puede obtener la rectificación de los datos personales propios que sean inexactos sin dilación indebida del responsable del tratamiento (art.16 RGPD). Teniendo en cuenta los fines del tratamiento, se tiene el derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional donde se deberá indicar a qué datos se refiere y la corrección que hay que realizar. Además, cuando sea necesario, se deberá acompañar la solicitud de la documentación que justifique la inexactitud o el carácter incompleto de los datos.

Derecho de oposición (art 18). El interesado tiene derecho a oponerse al tratamiento de sus datos personales basados en (art. 21 RGPD):

- el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al RT, o
- en la satisfacción de un interés legítimo del RT
- incluso la elaboración de perfiles sobre la base de lo anterior.

Este derecho puede ser ejercitado en cualquier momento. La consecuencia del ejercicio del derecho de oposición es que el RT dejará de tratar los datos personales:

Para conocer con más detalle estos derechos, consultad el documento de la AEPD:

<https://www.aepd.es/reglamento/derechos/index.html>

Los conocidos derechos **ARCO** (Acceso, Rectificación, Cancelación y Oposición) siguen existiendo. Existían en la LOPD anterior y ahora el derecho de Cancelación se ha ampliado con el derecho de supresión (art 15) o derecho al olvido y tres nuevos derechos.

Derecho de portabilidad.
Derecho de limitación
Derecho decisiones automatizadas

- salvo que acredite motivos legítimos imperiosos para el tratamiento que deberán prevalecer sobre los derechos y libertades del interesado, o
- para la formulación, ejercicio o la defensa de reclamaciones.

Si los datos personales son tratados con fines de mercadotecnia directa, el interesado tiene derecho a oponerse al tratamiento para dichos fines, inclusive a la elaboración de perfiles si está relacionado con dicha mercadotecnia directa, independientemente que sea el tratamiento inicial o ulterior.

Derecho de supresión (art 15). El derecho conocido como derecho "al olvido" es el de derecho de los interesados a que sus datos personales se supriman y dejen de tratarse en los supuestos contemplados en el RGPD (art. 17 RGPD). Se puede ejercitar este derecho ante el responsable (*) solicitando la supresión de sus datos de carácter personal cuando concurra alguna de las siguientes circunstancias:

- Si los 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 los datos personales se ha basado en el consentimiento que se prestó al responsable, y se retira el mismo, siempre que el citado tratamiento no se base en otra causa que lo legitime
- Si el interesado se ha opuesto al tratamiento de los datos personales al ejercitar el derecho de oposición en las siguientes circunstancias
 - El tratamiento del 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 los datos personales sean objeto de mercadotecnia directa, incluyendo la elaboración perfiles relacionada con la citada mercadotecnia
- Si los datos personales han sido tratados ilícitamente
- Si los 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 al 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).


(*) Este derecho de supresión se amplía de tal forma que el responsable del tratamiento que haya hecho públicos datos personales está 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.as.

El derecho al olvido ha sido una de las grandes novedades del RGPD.

DERECHO AL OLVIDO	
Los interesados tienen derecho a obtener la supresión de los datos	Los datos ya no sean necesarios para la finalidad para la que fueron recogidos
	Se revoque el consentimiento en el que se basaba el tratamiento
	El interesado se oponga al tratamiento
	Los datos se hayan tratado ilícitamente
	Los datos se tengan que suprimir para el cumplimiento de una obligación legal
	Los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información dirigidos a menores

Derecho al olvido

En el entorno Internet, cuando el RT haya hecho públicos los datos personales, está obligado a indicar a los RT que estén tratando dichos datos que supriman todo enlace a ellos, o las copias o réplicas de los datos. Para ello el RT deberá tomar las medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.

El derecho de supresión (derecho al olvido) implica el derecho a que tus datos personales se supriman así como todo enlace que contenga información personal en internet, o las copias o réplicas de tales datos y dejen de tratarse. 

Menores.

Cuando el interesado dio su consentimiento siendo niño, no siendo plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir los datos tratados, podrá ejercer también este derecho siendo ya adulto.

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 al 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.

El derecho al olvido ha sido una de las grandes novedades del RGPD.

5.1.2. Derecho a la limitación de tratamiento (art 16).

El derecho a la limitación del tratamiento (art. 18 RGPD) supone que a solicitud del interesado el RT deberá limitar el uso de los datos. Generalmente consiste en el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

Se corresponde con el artículo 18 del Reglamento.

Entre los métodos para limitar el tratamiento de datos personales el RGPD contempla los siguientes: trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, impedir el acceso de usuarios a los datos personales seleccionados, o retirar temporalmente los datos publicados de un sitio web. En principio, en los ficheros automatizados la limitación deberá realizarse por medios técnicos, imposibilitando cualquier operación de tratamiento ulterior o modificación de los datos. También deberá indicarse claramente en el sistema que el tratamiento está limitado.

Los supuestos en los que se puede solicitar la limitación del tratamiento presentan dos vertientes:

- Es posible solicitar la suspensión del tratamiento de los datos:
 - Cuando se impugne la exactitud de los datos personales, durante un plazo que permita al responsable su verificación
 - Cuando el interesado se haya opuesto al tratamiento de los 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 de los datos:
 - Cuando el tratamiento sea ilícito y el interesado se ha opuesto a la supresión de sus datos y en su lugar solicita la limitación de su uso
 - Cuando el RT 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

Durante el tiempo que dure la limitación el RT sólo podrá tratar los datos, más allá de su conservación en los siguientes casos:

- con el consentimiento del afectado;
- para la formulación, ejercicio o defensa de reclamaciones,
- para la protección de los derechos de otra persona física o jurídica;
- por razones de interés público.


5.1.3. Derecho a la portabilidad (art 17).

La finalidad de este nuevo derecho es reforzar aún más el control de los datos personales, de forma que cuando el tratamiento se efectúe por medios automatizados, el interesado pueda recibir los datos personales en un formato estructurado, de uso común, de lectura mecánica e interoperable, y pueda 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.

5.1.4. Derecho a no ser objeto de decisiones individuales automatizadas (art 22 apartado 1).

Se reconoce el derecho a no ser objeto de una decisión que evalúe aspectos personales relativos a una persona física, basada únicamente en el tratamiento automatizado y que produzca efectos jurídicos en ella o le afecte significativamente de modo similar. Una decisión tiene efectos jurídicos cuando sus derechos jurídicos se ven afectados. Por ejemplo, la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna.

Este derecho pretende garantizar que el interesado no sea objeto de una decisión basada únicamente en el tratamiento de sus datos, incluida la elaboración de perfiles 

Este tipo de tratamiento también se refiere a la elaboración de perfiles consistentes en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, especialmente cuando se analice o prediga aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, siempre que produzcan efectos jurídicos en él o le afecte de manera significativamente de manera similar.

Se considera que se elaboran perfiles cuando sus aspectos personales son evaluados para elaborar predicciones sobre su persona, incluso si no se toman decisiones. Por ejemplo, si una empresa u organización evalúa sus características (como la edad, el sexo, la altura) o le incluye en una categoría, significa que se está elaborando un perfil sobre usted.

Las decisiones basadas en algoritmos no pueden utilizar categorías especiales de datos, a menos que usted haya dado su consentimiento o que el proceso esté permitido por la legislación de la UE o nacional.

Información adicional

Artículos 21 y 22 y considerandos 71 y 72 del RGPD

Directrices del Grupo de trabajo del artículo 29 sobre decisiones individuales automatizadas y perfilado a los efectos del Reglamento (UE) 2016/679 (WP 251)

El RGPD contempla determinados supuestos de excepción, particularmente si:

1. la decisión es necesaria para la celebración o la ejecución de un contrato entre el interesado y el RT;
2. está autorizada expresamente por el Derecho de la UE o de los EM, siempre que se apliquen garantías apropiadas para salvaguardar los derechos y libertades del interesado.
3. se base en el consentimiento explícito del interesado.

En el primer y en el tercer supuesto el RGPD obliga a establecer una serie de salvaguardas para proteger los derechos y libertades de los interesados entre las cuales menciona: ofrecer información específica al interesado, el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de la evaluación y a impugnar la decisión.

En todo caso, con el fin de cumplir con los principios de lealtad y transparencia aplicables a los tratamientos de datos personales, el RT deberá utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles; aplicar las medidas técnicas y organizativas necesarias para garantizar que se corrigen los factores que introducen inexactitudes en los datos personales; reducir al máximo el riesgo de error; impedir los efectos discriminatorios en las personas físicas, o que den lugar a medidas que produzcan tal efecto.

En ningún caso las decisiones automatizadas podrán afectar a los menores.

Las decisiones automatizadas y la elaboración de perfiles sobre la base de las categorías especiales de datos únicamente podrán autorizarse en condiciones específicas.

Información adicional. Consultar

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

5.1.5. Limitaciones a los derechos.


El RGPD faculta que se puedan imponer restricciones o limitaciones en el ejercicio de los derechos establecidos en el mismo. Dichas limitaciones deberán establecerse por el Derecho de la UE o de los EM mediante una ley que deberá respetar los derechos y libertades fundamentales, además deberá ser una medida necesaria y proporcionada. Únicamente se podrán limitar los derechos de los interesados para:

- salvaguardar la seguridad del Estado, la defensa y la seguridad pública, incluida la protección de la vida humana en catástrofes naturales o de origen humano;
- prevenir, investigar, enjuiciar infracciones penales o la ejecución de las sanciones penales;
- cumplir objetivos importantes de interés público, en particular intereses económicos o financieros de la UE o de los EM, la sanidad pública o la seguridad social;
- prevenir, investigar, enjuiciar infracciones de normas deontológicas en las profesiones reguladas;

- protección del interesado o de los derechos o libertades de otros, incluida la protección social, la salud pública y los fines humanitarios;
- protección de la independencia judicial;
- la ejecución de demandas civiles.

Estas restricciones deberán ajustarse a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

5.2. Derechos digitales de los ciudadanos en internet

Incluye los arts. 79 a 82, 96 y 97 

- **Derecho a la neutralidad de Internet** (art. 80). Se reconoce a los usuarios de un derecho cuyo contenido se concreta en la obligación de los proveedores de servicios de Internet de proporcionar “una oferta transparente de servicios sin discriminación por motivos técnicos o económicos”
- **Derecho de acceso universal a Internet** (art. 81). Se establece, en síntesis que todos tienen derecho a acceder a Internet, que “se garantizará” que ese acceso será “universal, asequible, de calidad y no discriminatorio para toda la población”, incluidas las personas que cuenten “con necesidades especiales.” Y que el mismo “procurará la superación” de las brechas de género y generacional y atenderá a la realidad específica de los entornos rurales.
- **Derecho a la seguridad digital** (art. 82). Los “usuarios” tienen derecho “a la seguridad de las comunicaciones que transmitan y reciban a través de Internet”. En este caso se introduce una obligación a cargo de los proveedores de servicios de Internet: la de informar a los usuarios de sus derechos (se entiende que a este respecto, aunque no se aclara más).
- **Derecho al testamento digital** (art. 96). El art. 2.2 de la Ley Orgánica establece que la misma no será de aplicación “a los tratamientos de datos de personas fallecidas”. Pero ello sin perjuicio de lo previsto en el siguiente art. 3, que fija los criterios conforme a los cuales las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos, pueden acceder a los datos personales de aquél.

Concepto aparentemente mucho más amplio que el de “ciudadanos” al que se refiere el art. 18 de la CE


el art. 96 no regula una nueva forma testamentaria.

A diferencia de lo que pudiera sugerir su título, el art. 96 no regula una nueva forma testamentaria, diferente de las ya previstas en el Código Civil. Más bien viene a prever

un contenido específico de las disposiciones testamentarias que puede realizar una persona, referidas a un tipo concreto de “bienes” como son el contenido de la información relativa a la misma “gestionados por prestadores de servicios de la sociedad de la información”.

Finalmente, el artículo 97 (Políticas de impulso de los derechos digitales) establece la previsión de que el Gobierno de la Nación, en colaboración con las comunidades autónomas. Deberá elaborar dos documentos, el “Plan de Acceso a Internet” orientado 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. Y el “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.

5.3. Derechos relacionados con los menores

Incluye los arts. 83, 84, 92 y 97.2 (en parte) 

- **Derecho a la educación digital** (art. 83). Orientado a garantizar que el sistema educativo asegure “la plena inserción del alumnado en la sociedad digital” y su aprendizaje de un uso seguro y respetuoso con “la dignidad humana, 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” de los medios digitales.

Para ello se introduce un mandato directo a todas las “Administraciones educativas” a fin de que:

- 1) estas incluyan en el bloque de asignaturas de libre configuración la competencia digital 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.
- 2) Formar adecuadamente al profesorado en competencias digitales y para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.
- 3) Esa inclusión afecta igualmente a la enseñanza universitaria, “en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado”, que deberán garantizar

“la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet”.


- 4) 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.

- **Protección de los menores en Internet** (art. 84). Está a fin de reconocer dos obligaciones (*). Por un lado establece que los padres (y madres), tutores, curadores o representantes legales de los menores deberán procurar (“procurarán”) que los menores 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 derechos fundamentales. Por otro, el Ministerio Fiscal deberá instar (“instará”) las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, cuando la utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes “puedan implicar” una intromisión ilegítima en sus derechos fundamentales.
- **Protección de datos de los menores en Internet** (art. 92). Va dirigido a “los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad” y les impone la obligación de garantizar “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.

(*) Lo hace a través de un conjunto de expresiones muy imprecisas, que sin duda requerirán de la interpretación de los órganos judiciales para concretar su alcance

En los casos en que 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 art. 7 de esta Ley Orgánica.

5.4. Derechos relacionados con el ámbito laboral

Incluye los arts. 87 a 91 

Estos cinco artículos están dedicados específicamente al ámbito laboral (y, en paralelo, funcional o administrativo laboral), en una relación que se

debe complementar con lo dispuesto en las disposiciones finales 13.^a y 14.^a de la misma norma, que modifican respectivamente el Estatuto de los Trabajadores y el Estatuto Básico del Empleado Público

- **Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral (art. 87).** Se reconoce, en primer lugar, que tanto los trabajadores como 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”.

Se establece la obligación de los empleadores de “establecer criterios de utilización” de dichos dispositivos digitales, incluyendo la especificación de los usos autorizados y, en su caso, “la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados”. Igualmente deberán especificarse las posibilidades de acceso por el empleador al contenido de esos dispositivos digitales. De todo lo cual deberán ser informados los trabajadores.

Estándares mínimos de privacidad.

La previsión de que tales criterios de utilización deberán respetar unos estándares mínimos de privacidad de acuerdo “con los usos sociales y los derechos reconocidos constitucional y legalmente”, algo que parece subvertir el sistema de fuentes del Derecho previstas en el art. 1 del Código Civil.

- **Derecho a la desconexión digital en el ámbito laboral (art. 88).** Su contenido preciso no se define, aunque sí su finalidad. En su virtud “los trabajadores y los empleados públicos tendrán derecho a la desconexión digital” a fin de garantizar, fuera del tiempo de trabajo, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

Más concretamente, se añade que las modalidades de ejercicio de este derecho “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.

- **Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (art. 89).** Se aborda el complejo tema de la videovigilancia en el lugar de trabajo, permitiendo a los empleadores el tratamiento de las imágenes obtenidas, pero solo “para el ejercicio de las funciones de control de los trabajadores o los empleados públicos” previstas en la ley con los límites inherentes al mismo, y sin que dichos dispositivos puedan estar instalados en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos “tales como vestuarios, aseos, comedores y análogos”.

Solo se admite la utilización de sistemas de grabación de sonidos en el lugar de trabajo en caso de riesgos “relevantes” para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y respetando los principios de proporcionalidad e intervención mínima.

Este uso requerirá la previa información, “expresa, clara y concisa”, a los trabajadores y, en su caso, a sus representantes.

- **Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral** (art. 90). los sistemas de geolocalización son otros de los desarrollos tecnológicos que permiten un mayor control de la actividad de los trabajadores, que esta Ley ha venido a regular. La Ley autoriza a los empleadores el tratamiento de los datos obtenidos “a través de sistemas de geolocalización” solo para el ejercicio “de las funciones de control de los trabajadores o los empleados públicos” previstas en “su marco legal y con los límites inherentes al mismo” y previa información “expresa, clara e inequívoca” a los trabajadores o los empleados públicos y, en su caso, a sus representantes.
- **Derechos digitales en la negociación colectiva** (art. 91). la Ley asume en todo caso su condición de norma mínima, frente a la cual los convenios colectivos “podrán establecer garantías adicionales”.

5.5. Derechos relacionados con medios de comunicación


Incluye los arts. 85 y 86 

- **Derecho de rectificación en Internet** (art. 85). Se comienza reconociendo con claridad que “Todos tienen derecho a la libertad de expresión en Internet”. Así pues, “los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación”, según “los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación”.

La atención a la solicitud de rectificación dirigida contra un medio de comunicación digital deberá ir acompañada de la publicación en lugar visible de sus archivos digitales “de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo”.

- **Derecho a la actualización de informaciones en medios de comunicación digitales** (art. 86). Este artículo reconoce el derecho de “toda persona” a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización visible junto a las noticias que le conciernen “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” y, en particular, cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado por una decisión judicial posterior.

5.6. Derecho al olvido en Internet


Derecho al olvido en internet: arts. 93 y 94 

Derecho al olvido en búsquedas de Internet (art. 93)

Se establece un derecho de “toda persona” frente a los motores de búsqueda en Internet y en el art. 94 frente a los “servicios de redes sociales y servicios de la sociedad de la información equivalentes”. Se trata de un derecho ejercible frente a un buscador, pero no frente a un medio de comunicación

- **Derecho al olvido en internet** (art. 93). Los motores de búsqueda deberán eliminar de las listas de resultados “que se obtuvieran tras una búsqueda efectuada a partir de su nombre”, de 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”, todo ello teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.
- **Derecho al olvido en servicios de redes sociales y servicios equivalentes** (art. 94). Se reconoce el derecho de “toda persona” a que sean suprimidos, “a su simple solicitud”, los datos personales publicado en las redes sociales, ya los hubiera facilitado ella misma, ya “hubiesen sido facilitados por terceros”, en este caso “cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo” o 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”.

5.7. Derecho a la portabilidad

Derecho a la portabilidad en las redes sociales: art. 95 

- **Derecho de portabilidad en servicios de redes sociales y servicios equivalentes** (art. 95). Se trata de una modalidad específica de un derecho para un ámbito concreto. Se trata del derecho a la portabilidad de los datos que le incumban y que haya facilitado a un responsable de tratamiento, regulado en el art. 20 del RGPD, y cuyo ejercicio, según el art. 17 de la Ley Orgánica se realizará “de acuerdo con lo establecido” en dicho art. 20, de los usuarios de servicios de redes sociales y de servicios equivalentes.

Para saber más puedes consultar la Guía del GT29 sobre portabilidad, aquí http://ec.europa.eu/newsroom/document.cfm?doc_id=44099

En virtud de este artículo, dichos usuarios “tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios”, así como a que tales los prestadores “los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible”.

El derecho a la portabilidad de los datos (art. 20 RGPD) se configura como una forma de acceso a los datos personales que permite a los interesados recibir sus datos personales en formato estructurado, de uso común, de lectura mecánica e interoperable. Además, el interesado tiene derecho a que los datos personales se transmitan directamente de un RT a otro RT, siempre que sea técnicamente posible. No obstante, el derecho del interesado a que sus datos se transmitan a otro RT no obliga al RT a adoptar o mantener sistemas de tratamiento técnicamente compatibles.

Este derecho sólo será aplicable a los tratamientos automatizados y únicamente en dos supuestos:

- cuando el interesado haya facilitado los datos personales dando su consentimiento o,
- cuando el tratamiento sea necesario para la ejecución de un contrato.

No se aplica en relación a:

- A los datos de terceras personas que un interesado haya facilitado a un responsable.
- En caso de que el interesado haya solicitado la portabilidad de datos que le incumban pero que hayan sido proporcionados al responsable por terceros.

6. Responsabilidad proactiva

Una de las principales novedades y concepto esencial que presenta el Reglamento General de Protección de Datos, es el principio de responsabilidad proactiva o responsabilidad activa (*accountability*). En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión. Ahora corresponde a las organizaciones la responsabilidad de identificar los propios focos de riesgo y de elegir medidas adecuadas para mitigarlo.

Se refiere al concepto anglosajón de responsabilidad y transparencia (*accountability*).

En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo. !

Toda organización sujeta al reglamento debe estar en disposición de acreditar ante cualquier requerimiento del organismo competente que:

- Ha evaluado, y en caso necesario, rediseñado adecuadamente sus tratamientos de datos personales.
- Las medidas de seguridad implementadas son adecuadas y eficaces.
- Se aplica una política interna en materia de privacidad con obligaciones claras, acciones concretas anudadas a cada una, y se han designado responsables de su cumplimiento.
- Exige ese mismo cumplimiento responsable a sus encargados de tratamientos y cadena de subcontratación.


La adopción de una política de protección de datos personales por parte de la organización que va a tratar los datos consiste en una serie de medidas e instrumentos para garantizar una protección óptima de los datos personales tratados (*). Las más importantes son:

- **Análisis de los riesgos** que suponen los tratamientos de datos y cuáles son las medidas de seguridad a aplicar para prevenirlo y corregirlos en caso necesario.
- **Registro de actividades de tratamiento**, que busca analizar qué información se gestiona, quienes son los interesados, que aplicaciones tendrán estos tratamientos, que cesiones están previstas, etc.

- **Protección desde el diseño y por defecto.** Eso implica que la puesta en marcha de una actividad profesional o empresarial, no puede llevarse a cabo sin haber establecido y analizado los datos que se van a gestionar.
- **Las medidas de seguridad** a implantar, que deberán ser analizadas y monitorizadas de forma constante (**).
- **Notificaciones de brechas de seguridad**, que tendrán que ser comunicadas antes de 72 horas a las autoridades pertinentes.
- **Evaluación de Impacto en la protección de datos (EIPD)**, previa a la puesta en marcha del tratamiento. En aquellos casos en que los datos puedan suponer un riesgo para los derechos y libertades de los usuarios. Además, las Evaluaciones de Impacto sobre la protección de los datos (EIPD) permiten identificar los riesgos asociados al tratamiento y la adopción de medidas para su prevención
- **La evaluación de prácticas y la implementación de procedimientos**, incluye la notificación de las Violaciones de Seguridad de los datos o la gestión de solicitudes de ejercicios de derechos de los interesados.
- **Mantener una documentación** interna que asegure la trazabilidad de las medidas adoptadas.
- **El nombramiento de la figura del Delegado de Protección de Datos.**

A fin de cumplir con el principio de responsabilidad proactiva, la organización lo lleva a cabo a través de la figura del responsable del tratamiento. Así pues, el responsable del tratamiento de datos tiene la obligación de aplicar las medidas técnicas y organizativas apropiadas a fin de poder garantizar una protección óptima y de poder demostrar que el tratamiento de datos personales es conforme con el Reglamento. Es decir, no basta con cumplir con la normativa de protección de datos, también hay que poder demostrar que se está cumpliendo con la normativa. Para ello, el responsable del tratamiento de datos deberá establecer procedimientos a través de los cuales:

- Pueda garantizar la aplicación de la normativa de protección de datos.
- Pueda demostrar frente a terceros la efectiva aplicación y el cumplimiento de la normativa de protección de datos.

Este principio se define como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y estar en condiciones de acreditar que el tratamiento es conforme con el Reglamento (art.24.1). 

(*) Una diferencia sustancial con la antigua ley es que no se especifican de forma concreta qué medidas se tienen que implantar, con lo cual deja a decisión de cada entidad como y de qué manera se van a proteger los datos.

(**) Mediante la ejecución de estas medidas (no todas son obligatorias para todas las entidades), se garantiza la capacidad del responsable del tratamiento de datos de demostrar y proporcionar evidencias del cumplimiento de protección de datos.

En el apartado de las medidas técnicas y organizativas se ven con detalle.

Este principio también viene recogido en el artículo 5 apartado 2 del RGPD: “El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)”.

7. Figuras

La normativa establece la existencia de la figura del responsable, del encargado y del delegado de tratamiento de datos como unos perfiles que desempeñan un papel muy relevante para la correcta aplicación del reglamento.

En los siguientes apartados detallamos estas figuras.

- **Responsable del tratamiento (RT)** de los datos es aquella persona física o jurídica, de naturaleza pública o privada, o bien el órgano administrativo que decide sobre la finalidad, contenido y uso del tratamiento de los datos personales.
- **Encargado de tratamiento (ET)** es la persona física o jurídica o el órgano administrativo que realiza el tratamiento de los datos por cuenta del responsable.
- **Delegado de Protección de Datos (DPD)** es quien, entre otras funciones, debe supervisar el cumplimiento de la normativa en materia de protección de datos personales.

A menudo se usa el término anglosajón DPO, Data Protection Officer.

ENCARGADO DEL TRATAMIENTO

Persona física o jurídica, de naturaleza pública o privada, o bien el órgano administrativo que en el ejercicio de su actividad trata con datos personales.

Por ley tiene la obligación de determinar como se tratan y gestionan los datos personales de su entidad, haciéndose responsable de la creación y gestión de los ficheros

RESPONSABLE DEL TRATAMIENTO

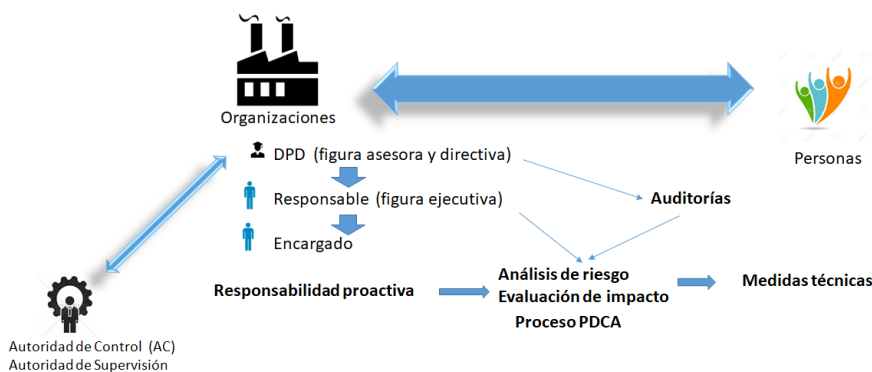
Persona física o jurídica, de naturaleza pública o privada, o bien el órgano administrativo que en el ejercicio de su actividad trata con datos de carácter personal que son responsabilidad del Responsable del Tratamiento

DPD

Ayuda al Responsable o al Encargado del Tratamiento. Es un profesional con conocimientos especializados de la normativa y práctica en materia de protección de datos

Los DPD pueden ser empleados o no del Responsable del Tratamiento, pero deben estar en condiciones de realizar sus funciones de manera independiente

Diferencia entre las figuras



Esquema de la relación entre todos los elementos del reglamento

7.1. Responsable de tratamiento (RT)

El artículo 4.7 del Reglamento define al responsable del tratamiento o responsable como "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".

La figura del RT está regulada en el TÍTULO V (arts. 28 a 37) de la Ley.

El RT decide sobre el tratamiento de los datos; con qué finalidad se van a utilizar, con quién se van a compartir, durante cuánto tiempo se van a conservar, etc.

Se trata de una definición muy amplia, ya que cualquier persona física o jurídica, en los términos indicados, que decida sobre el tratamiento de los datos personales será considerada responsable del tratamiento

En relación con la definición de responsable...

hay que considerar que el Grupo de Trabajo del Artículo 29 (GT29), que se integró desde el 25 de mayo de 2018 en el Comité Europeo de Protección de Datos (CEPD), publicó un relevante dictamen sobre esta figura. Se trata del Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", WP 169, adoptado el 16 de febrero de 2010. Si bien el dictamen fue emitido antes del RGPD, en lo fundamental sigue siendo aplicable.

"El papel primero y primordial del concepto de responsable del tratamiento es determinar quién debe asumir la responsabilidad del cumplimiento de las normas sobre protección de datos y de qué manera

los interesados pueden ejercer sus derechos en la práctica. En otras palabras, debe asignar la responsabilidad." !

7.1.1 Funciones, obligaciones y responsabilidades

Algunas de ellas se encuentran descritas en el artículo 32 del Reglamento.

Su condición de Responsable hace que esté sujeto a los requerimientos establecidos en la normativa y que, en consecuencia, tenga que observar cuantas obligaciones disponga el Reglamento General de Protección de Datos.

El Responsable del Tratamiento decide la creación del fichero, la finalidad del tratamiento, así como el contenido y el uso de los datos almacenados en ese fichero. Esta responsabilidad debe desarrollarla durante toda la “vida” del dato, es decir, desde que este entra a formar parte del sistema de información hasta la eliminación del mismo.

El Responsable debe informar y obtener consentimiento para proceder a la recogida de los datos personales.

También deberá determinar 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. Los trabajadores que realizan el tratamiento de los datos personales en una organización lo hacen en cumplimiento de las funciones que ejerce el responsable del tratamiento

El responsable debe determinar y aplicar las medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos de carácter personal y evitar así su alteración, pérdida, tratamiento o acceso no autorizado. Además debe estar en condiciones de demostrar la conformidad de las actividades de tratamiento con el Reglamento, incluida la eficacia de las medidas. El hecho de no aplicar dichas medidas es sancionable.

Algunas de las medidas (artículo 32) pueden ser:

- a) La seudoanonimización y el cifrado de datos personales;
- b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico;
- d) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Establecerá la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado con referencia a la naturaleza, el ámbito, el contexto y el fin que entraña el tratamiento que pretende realizar para los derechos y libertades para las personas físicas. El riesgo deberá ponderarse mediante una


evaluación objetiva que determine si las operaciones suponen un riesgo y si el riesgo es alto.

Los riesgos de gravedad y probabilidad variables pueden provocar daños y perjuicios, en particular en los casos en que:

- puedan dar lugar a problemas de discriminación, usurpación de identidad o fraude, daño en la reputación, pérdida de confidencialidad o reversión no autorizada de la seudonimización; en los casos en que se prive a los interesados de sus derechos o libertades o se les impida ejercer el derecho sobre sus datos personales;
- los datos revelen el origen étnico o racial, opiniones políticas, religión, militancia en sindicatos, datos genéticos, etc.;
- se evalúen aspectos personales, con el fin de crear o utilizar perfiles personales;
- se traten datos personales de personas vulnerables, en particular de niños;
- el tratamiento implique gran cantidad de datos personales y afecte a un gran número de interesados.

Con el objetivo de demostrar que se han adoptado las medidas técnicas y organizativas adecuadas, el RT debe adoptar políticas internas y aplicar medidas.

La figura del responsable del tratamiento es fundamental dentro del RGPD. Debe poder demostrar frente a terceros la efectiva aplicación y el cumplimiento de la normativa de protección de datos.

Deberá elegir un encargado del tratamiento que ofrezca garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas, así como de verificar que se cumplen las medidas adoptadas. 

Es decir...

Siempre que, como responsable, tengas que compartir datos de clientes, empleados, suscriptores, etc. con otra empresa o un autónomo para que realicen un trabajo para ti que implique el tratamiento de estos datos, estamos hablando de una relación de encargo de tratamiento que implica la presencia de un contrato de encargo que defina las condiciones del tratamiento, finalidades, obligaciones, etc.

Los responsables habrán de elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento.

Esta previsión se extiende también a los encargados cuando subcontraten operaciones de tratamiento con otros subencargados.

7.1.2. Tratamiento que no requiere identificación.

Si los datos personales tratados por un RT no permiten identificar a una persona física, el RT no está obligado a obtener o tratar información adicional para identificar al interesado con la única finalidad de cumplir con el

RGPD. En tal caso, el RT ha de ser capaz de demostrar que no puede identificar al interesado y, cuando sea posible, deberá comunicárselo. En este supuesto no se aplicarán las disposiciones relativas al ejercicio de derechos del interesado.

Sin embargo, cuando con motivo del ejercicio de sus derechos el interesado facilita al RT información adicional, este no podrá negarse a recibir tal información y, en consecuencia, no podrá negarse a atender la solicitud de ejercicio de derechos formulada por el interesado.

La identificación incluye la identificación digital del interesado, por ejemplo, las credenciales empleadas por el interesado para abrir una sesión en el servicio en línea ofrecido por el RT.

7.2. Encargado de tratamiento (ET)

El encargado de tratamiento es aquella persona física o jurídica, autoridad pública o servicio que, solo o conjuntamente con otros, trata datos de carácter personal por cuenta del responsable de tratamiento, pues existe una relación jurídica que le vincula con el mismo. Es decir, que el tratamiento que realice un ET deberá regirse por un contrato u otro acto jurídico que vincule al encargado con el RT y deberá fijar un contenido mínimo. En el mismo debe establecerse el objeto, duración, la naturaleza y finalidad del tratamiento, el tipo de datos personales y categorías de interesados, así como las obligaciones y derechos del responsable, todo ello habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que se lleve a cabo.

Por ejemplo...

incluye, entre otros, a empresas de marketing, gestorías contables, empresas de hosting, empresas de servicios informáticos, etc.

Normalmente, se trata de un tercero que realiza determinadas tareas por encargo del responsable.

La figura del ET está regulada en el TÍTULO V (arts. 28 a 37) de la Ley.

7.2.1 Funciones, obligaciones y responsabilidades

El acuerdo o acto que se suscriba entre el responsable y el encargado del tratamiento deberá contener al menos las siguientes obligaciones y responsabilidades para el encargado:

- Realizar el tratamiento siguiendo las instrucciones documentadas del responsable, inclusive en relación a las transferencias de datos personales a un tercer país o una organización internacional.
- Garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

- Que se tomarán las medidas de seguridad necesarias, conforme a lo dispuesto en el RGPD. El ET deberá aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
- No aplicará ni utilizará los datos con un fin distinto al que figure en el contrato.
- No comunicará los datos, ni siquiera para su conservación, a otras personas.
- Expondrá qué hará con los datos una vez finalizado el servicio correspondiente.
- Respetar las condiciones indicadas en el RGPD para subcontratar con otro encargado de tratamiento.
- Asistir al responsable para que éste pueda dar cumplimiento a su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados. Asimismo, ayudará al responsable a garantizar el cumplimiento de las obligaciones previstas en el RGPD, esto es, respecto de la seguridad de los datos y la evaluación de impacto sobre la protección de datos.
- Facilitar al responsable la información necesaria para demostrar el cumplimiento de todas las obligaciones y así permitir y contribuir a la realización de auditorías, incluidas las inspecciones.
- Deber de informar de manera inmediata al responsable en caso que alguna de las instrucciones que le sean trasladadas infringe el Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los estados miembros.

Para que el encargado del tratamiento pueda acceder a los datos no es necesario el consentimiento de los afectados, es decir, de las personas cuyos datos se tratan siempre que exista el contrato de encargo mencionado.

Finalizado el tratamiento, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que se requiera la conservación de dichos datos en virtud de la normativa vigente.

7.3. Delegado de protección de datos (DPD)

La figura del Delegado de protección de datos (DPD o DPO en inglés) es otra de las novedades del RGPD, si bien, algunos países miembros de la UE, como Alemania, ya contaban con dicha figura antes de la aprobación del RGPD.

El DPD se configura como la persona con conocimientos especializados en Derecho, (no necesariamente un licenciado en Derecho), la normativa y la práctica en materia de protección de datos. Además, en función de las operaciones de tratamiento que lleve a cabo la organización, el DPD deberá tener distinto nivel de conocimientos especializados.

La figura del DPD está regulada en los arts. 34 a 37) de la Ley.

Se debe garantizar su independencia dentro de la organización, debiendo evitarse cualquier conflicto de intereses (*). Cuando se trate de un DPD externo a la organización, la relación jurídica entre ambos se basará en un contrato de servicios. En determinados supuestos también es posible designar un único DPD para varias organizaciones (art. 37. 2 y 3 DPD). Es obligación del RT publicar los datos del DPD y, además, comunicarlos a la autoridad de control. Para preservar su independencia no deberá recibir ninguna instrucción del RT (o del ET) en el desempeño de sus funciones, ni podrá ser destituido o sancionado por motivos relacionados en el desempeño de sus funciones.

La posición del DPD en la organización deberá estar al nivel de otros directores, ya que el RGPD señala que éste rendirá cuentas directamente al más alto nivel jerárquico.

Otro aspecto a tener en cuenta es la posibilidad de que se produzca un conflicto de intereses como consecuencia del ejercicio de funciones como DPD. El Reglamento permite que el DPD pueda desempeñar otras funciones en la organización, si bien, únicamente podrá hacerlo si no se produce un conflicto de intereses (art. 38.6 RGPD) (*).


Por ejemplo...

En determinadas situaciones queda claro sin lugar a dudas que se produce dicho conflicto. Sería el caso de un DPD que ejerza otra posición en la organización en la cual pueda determinar finalidades o medios del tratamiento. Un ejemplo claro sería un DPD que, a su vez, es director de máquetin.

(*) Por lo tanto, desempeñarán sus funciones de manera independiente.

Los DPD podrán ser o no empleados del RT o ET.

(*) Para determinar si existe conflicto de intereses es necesario estudiar caso por caso, pues la casuística puede ser muy variada.

El delegado de protección de datos es la persona que actúa como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. 

Además es el responsable de garantizar que se cumpla con la normativa de protección de datos dentro de la empresa u organización.

Existe un registro oficial de delegados de protección de datos certificados de diferentes entidades.

Por último, los Responsables y Encargados de Tratamiento, comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos y, 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 encuentre la empresa obligada como en el caso en que la designación sea voluntaria.

7.3.1 Funciones, obligaciones y responsabilidades

- **Asesorar y asesorar** al responsable o al Encargado de Tratamiento
- **Inspeccionar los procedimientos** relacionados con el cumplimiento del RGPD y emitir recomendaciones en el ámbito de sus competencias.
- **Informar y asesorar** a los empleados que se ocupen del tratamiento acerca de las obligaciones que les incumben en virtud del RGPD, así como de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- **Supervisar el cumplimiento del Reglamento.** Es decir, de las normas incluidas en el RGPD, así como 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.
- **Asesorar respecto de la evaluación de impacto** relativa a la protección de datos al que se enfrenta la organización y supervisar su aplicación. Esto es debido a que con el nuevo Reglamento ya no hay que inscribir los ficheros de datos en la AEPD ni los datos personales están sujetos, como en la antigua ley, a los niveles de seguridad alta, media o baja.
- **Supervisar la aplicación de las normas** por el encargado del tratamiento en materia de protección de datos personales. Dentro de este apartado se incluyen: asignación de responsabilidades, formación del personal y auditorías correspondientes.
- **Actuar como representante** de la organización ante la Agencia Española de Protección de Datos (AEPD) en lo relativo al tratamiento de datos y la realización de consultas.
- **Velar por la conservación de la documentación.**
- **Supervisar la documentación**, notificación y comunicación de las violaciones de datos personales.
- **Supervisar la respuesta a las solicitudes de la autoridad de control** y cooperar con ella por solicitud de las mismas o por iniciativa propia.
- **Ejercer de punto de contacto con la autoridad de control** sobre cuestiones relacionadas con el tratamiento.

Las funciones mínimas del DPD están contempladas en el art. 39 RGPD.

- **Cooperar** con la autoridad de control.
- **Actuar como punto de contacto** para cuestiones relativas al tratamiento, tanto respecto a la autoridad de control como a los interesados.
- **Intermediario.** En caso de reclamación ante las autoridades de protección de datos a una organización, el DPD ejerce un papel órgano intermedio de control.

El Delegado de Protección de Datos velará porque se cumpla la normativa de protección de datos en las organizaciones y tendrá estrecha relación con las autoridades correspondientes a esta legislación.



Documentación relacionada

epígrafe 4º del documento elaborado por el GT Art.29 Guidelines on Data Protection Officers

https://ec.europa.eu/newsroom/document.cfm?doc_id=44100

GT Art.29 Guidelines on Data Protection Officers

http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf

7.3.2 Obligatoriedad de la figura del DPD

EL DPO no es obligatorio para todas las empresas. Su obligatoriedad es necesaria:

- Cuando el tratamiento lo lleva a cabo una Autoridad u Organismo Público, excepto los tribunales cuando actúen en el ejercicio de la función judicial
- En los tratamientos a gran escala que por su naturaleza, alcance y/o fines requieran una observación habitual y sistemática de interesados, como la creación de perfiles.
- Cuando las actividades principales del responsable o el Encargado de Tratamiento consisten en el tratamiento a gran escala de categorías especiales de datos o datos personales relacionados con condenas y delitos penales.
- Si la empresa u organización cuanta con más de 250 trabajadores. De este modo, las entidades con menos de 250 trabajadores estarán exentas de incorporar al DPO, a menos que el tratamiento de datos que se realice dentro de la organización pueda entrañar un riesgo para los derechos y libertades de los interesados, o incluya categorías de datos especiales o relativos a condenas e infracciones penales.

El RGPD exige que se nombre un DPD en los casos contemplados en el art. 37.

7.3.3 Organizaciones que deben tener DPD

- Los colegios profesionales y sus consejos generales
- Los centros docentes

- Las entidades que exploten redes y presten servicios de comunicaciones electrónicas, incluyéndose las compañías telefónicas y los proveedores de acceso a internet
- Los prestadores de servicios de la sociedad de la Información destacando los operadores de telecomunicaciones, proveedores de acceso a internet, los portales, motores de búsqueda y cualquier sujeto que disponga de un sitio en internet
- Las entidades de crédito, incluyendo los bancos, cajas de ahorro, cooperativas de crédito y el instituto de crédito oficial
- Los establecimientos financieros de crédito y aquellas empresas que, sin tener la consideración de entidad de crédito y previa autorización del ministerio de Economía y Competitividad, se dediquen con carácter profesional a la concesión de préstamos y créditos, el arrendamiento financiero o la concesión de avales y garantías.
- Las entidades aseguradoras y reaseguradoras
- Las empresas de servicios de inversión como las sociedades de valores, las agencias de valores, las sociedades gestoras de carteras y las empresas de asesoramiento financiero
- Los distribuidores y comercializadores de energía eléctrica y de gas natural
- Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito de los ficheros comunes para la gestión y prevención del fraude incluyendo a los responsables de los ficheros regulados por la Ley de Prevención del Blanqueo de Capitales y Financiación del Terrorismo
- Las entidades que desarrollen actividades de publicidad y prospección comercial, es decir aquellas empresas 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
- Los centros sanitarios
- Las entidades que tengan como uno de sus objetos la emisión de informes comerciales acerca de personas y empresas

- Los operadores que desarrollen la actividad de juego, siempre que la actividad se realice través de canales electrónicos, informáticos, telemáticos e interactivos
- Quienes desempeñen las actividades de seguridad privada, incluidos los vigilantes de seguridad y su especialidad de vigilantes de explosivos, los escoltas privados, los guardas rurales y su especialidad de guardas de caza y guardapescas marítimos, los jefes de seguridad, los directores de seguridad y los detectives privados

8. Medidas técnicas y organizativas

El RGPD establece un catálogo de las medidas que los responsables, y en ocasiones los encargados, deben aplicar para garantizar que los tratamientos que realizan son conformes con el Reglamento y estar en condiciones de demostrarlo.

En cuanto a la metodología del análisis de riesgos a utilizar, el RGPD no menciona nada. Sin embargo, es lógico que las organizaciones de gran tamaño o las que realicen tratamientos a gran escala utilicen algunas de las metodologías de análisis de riesgos existentes. Sin embargo, en las organizaciones de menor tamaño, siempre que no realicen tratamientos complejos, ni traten categorías especiales de datos, puede que no sea necesario un análisis formal. En cualquier caso, al evaluar la adecuación del nivel de seguridad se tendrán en cuenta los riesgos del tratamiento, en particular las consecuencias de la destrucción, pérdida o alteración accidental o ilícita de los datos personales, y la comunicación o acceso no autorizados de los mismos.

Dado que el RGPD exige que el RT y el ET estén en disposición de demostrar que han adoptado medidas de seguridad adecuadas, una forma de poder demostrarlo es mediante la adhesión a códigos de conducta aprobados o a alguna certificación aprobada conforme al RGPD (art. 32.3 RGPD).

Finalmente, el RT y el ET deberán tomar medidas que garanticen que cualquier empleado con acceso a datos solo pueda tratarlos siguiendo las instrucciones del RT.

8.1. Análisis de riesgos.

El nuevo GDPR exige que todas las organizaciones que tratan datos realicen un análisis de riesgo de sus tratamientos para poder determinar qué medidas han de aplicar y cómo hacerlo.

El tipo de análisis variará en función de:

- los tipos de tratamiento,
- la naturaleza de los datos,
- el número de interesados afectados,
- la cantidad y variedad de tratamientos que una misma organización lleve a cabo.

Estos análisis pueden ser muy simples en entidades que no llevan a cabo más que unos pocos tratamientos sencillos que no impliquen, por ejemplo datos

sensibles. Pero pueden resultar más complejos en entidades que desarrollen muchos tratamientos, que afecten a gran cantidad de interesados o que por sus características requieran de una valoración cuidadosa de sus riesgos.

8.2. Registro de actividades de tratamiento (RAT)

En la antigua LOPD, se establecía la obligatoriedad de elaborar un Documento de Seguridad por parte de los responsables de los ficheros. Este documento debía identificar los ficheros y especificar las medidas técnicas y organizativas en función los ficheros. Este documento debía de ser de obligado cumplimiento por parte del personal con acceso a los sistemas de información. Las medidas de seguridad podían de tipo bajo, medio o alto. Además existía la obligación de notificar y registrar los ficheros que contenían datos personales ante la autoridad de control.

Con la llegada del RGPD, desaparece el Documento de Seguridad, igual que desaparecen los ficheros y el registro de los mismos ante la autoridad de control. En su lugar, se exige al responsable del tratamiento y en su caso, del encargado, un registro de actividades de tratamiento que describa esas actividades y las medidas de seguridad aplicadas. En lugar de establecerse por niveles (alto-medio-bajo) el RGPD establece que esas medidas serán establecidas en función al riesgo detectado, para lo cual se exige un análisis de riesgo previo al tratamiento.

Tienen obligación de mantener un registro de actividades de tratamiento las empresas u organizaciones a partir de 250 trabajadores, también las que emplean menos de 250 trabajadores cuando:


- realizan tratamientos que puedan conllevar riesgos para los derechos o las libertades de los interesados, cuando el tratamiento no sea ocasional, o
- incluyan en los tratamientos categorías especiales de datos o datos relativos a condenas o infracciones penales.

Tanto los RT como los ET están obligados a cooperar con la autoridad de control y a poner a disposición de esta los registros, de modo que puedan supervisar las operaciones.

El registro de actividades de tratamiento o RAT, deberá incluir:

- Nombre y datos de contacto del responsable y, en su caso, del responsable, representante del responsable y del delegado de protección de datos.
- Finalidades del tratamiento.

- Descripción de categorías de interesados y categoría de datos personales tratados.
- Descripción de categorías de destinatarios a quienes se comunicaron o comunicarán datos personales, así como terceros países u organizaciones internacionales.
- Transferencias de datos personales a un tercer país o una organización internacional. incluida la identificación del país u organización internacional y, en su caso la documentación de las garantías adecuadas.
- Cuando sea posible, plazos previstos para la supresión de los datos, cuando sea posible.
- Descripción general de las medidas técnicas y organizativas de seguridad.

El RAT incluye básicamente, la declaración de ficheros y el documento de seguridad; es una fusión de ambos. (art. 30.2 RGPD) 

8.3. Privacidad desde el diseño y por defecto.

La protección de datos desde el diseño y por defecto es una cuestión de estrategia que, tanto el responsable como el encargado del tratamiento, deben tener en consideración para asegurar el derecho a la protección de datos mediante la adopción de medidas que consideren al titular de los datos personales, desde el principio en el que se genera una idea que pueda dar lugar a una aplicación, servicio o producto. A fin de poder demostrar la conformidad con el RGPD, el RT deberá adoptar políticas internas y aplicar medidas que cumplan los principios de protección de datos desde el diseño y por defecto.

La privacidad desde el diseño implica que cuando se está diseñando un producto o un servicio se tendrá en cuenta la protección de los datos personales como un elemento más a tomar en consideración. Teniendo en cuenta lo anterior, en el momento de determinar los medios de tratamiento como en el momento del tratamiento, el RT deberá aplicar medidas técnicas y organizativas apropiadas (art. 25.1 RGPD) a fin de:

- proteger los derechos de los interesados, como la seudonimización de los datos que deberá aplicarse lo antes posible.
- aplicar los principios de protección de datos, como la minimización de los datos tratados;
- integrar las garantías necesarias en el tratamiento.

A la hora de implementar dichas medidas, el RT tendrá en cuenta el estado de la técnica, el coste de la aplicación, la naturaleza, ámbito, contexto y

finés del tratamiento; evaluando los riesgos que entraña el tratamiento para los derechos y libertades del interesado.

Además, deberá garantizar que por defecto:

- que únicamente se traten los datos personales necesarios para cada uno de los fines específicos del tratamiento. Obligación que se aplicará a la cantidad de datos recogidos, al plazo de conservación y a su accesibilidad.
- que los datos no sean accesibles a un número indeterminado de personas sin la intervención de la persona.
- la transparencia de las funciones y del tratamiento permitiendo a los interesados supervisar el tratamiento de datos y al RT crear y mejorar elementos de seguridad.

Al desarrollar, diseñar, seleccionar o usar aplicaciones, servicios y productos que traten datos personales, los diseñadores de tales productos deberían tener en cuenta la protección de los datos personales, a fin de que el RT pueda cumplir con las obligaciones que les impone el RGPD. Un mecanismo para acreditar el cumplimiento podría ser el uso de certificaciones de organismos acreditados.

8.4. Evaluación de Impacto relativa a la protección de datos y consulta previa.

Cuando sea probable que un tratamiento, especialmente si se utilizan nuevas tecnologías, por su naturaleza, alcance, contexto o fines entrañe un alto riesgo para los derechos y libertades de las personas físicas, el RT realizará una evaluación de impacto de las operaciones de tratamiento antes de proceder a tratar los datos (art.35 RGPD). Se deberá evaluar también el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo (Considerando 84 del GDPR).

Esta evaluación se debe realizar con el asesoramiento del DPO (Data Protection Officer).

Se requerirá realizar una evaluación de impacto (EIPD) cuando el tratamiento implique un alto riesgo para los derechos y libertades de las personas físicas, en particular en caso de:

- evaluación sistemática y exhaustiva de aspectos personales de personas físicas, como en la elaboración de perfiles, sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
- tratamiento a gran escala de categorías especiales de datos o de los datos relativos a condenas e infracciones penales;
- control a gran escala de una zona de acceso público.

La EIPD deberá incluir como mínimo:

- La descripción detallada de lo siguiente:
 - descripción sistemática de las operaciones de tratamiento previstas y de los fines de tratamiento y, cuando proceda el interés legítimo del RT.
 - las distintas finalidades del tratamiento
 - el interés legítimo perseguido por el responsable;
- una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento respecto a su finalidad;
- evaluación de los riesgos para los derechos y libertades de los interesados;
- las medidas previstas para afrontar los riesgos, en particular las garantías, las medidas de seguridad y los mecanismos que garanticen la protección de datos personales.

Si una EIPD muestra un alto riesgo y el RT no puede mitigarse con las medidas adecuadas deberá consultar a la autoridad de control antes del tratamiento (art.36 RGPD).

8.5. Medidas de seguridad

El Responsable del Tratamiento debe evaluar la adecuación del nivel de seguridad a aplicar en el tratamiento de datos personales, teniendo en cuenta los riesgos que presente el tratamiento de dichos datos. el RGPD no recoge ni prevé desarrollar un catálogo de medidas de seguridad concretas.

A cada riesgo previamente identificado y evaluado debemos establecerle un control que nos lleve a poder medir – y acreditar - que hemos puesto esa medida de control y que funciona al objeto de minimizar la probabilidad de que el riesgo ocurra, con el consiguiente impacto asociado

De acuerdo con el RGPD la adopción de medidas se realizará en función del riesgo para los derechos y libertades de los interesados, teniendo en cuenta el estado de la tecnología y los costes de su aplicación, la naturaleza, alcance y contexto del tratamiento. Esto implica que para determinar las medidas de seguridad aplicables, los RT deberán realizar un análisis de riesgo para cada tratamiento que realicen.

Desde el punto de vista técnico, las medidas engloban un conjunto de actividades y procesos destinados a evitar la sustracción, pérdida, deterioro o destrucción de datos de carácter personal tratados. Algunos de estos procesos pueden ser:

Estas pueden ser preventivas y reactivas. Siempre tienen como fin último la confidencialidad, la disponibilidad y la integridad de la información (además obstaculizan una fuga de datos o brecha de seguridad).

Esta lista proporciona medidas que son aplicables y necesarias a cualquier organización, pero será esta la que elabore la lista completa en función de sus necesidades.


- Identificación y Autenticación de Usuarios.
- Control de acceso.
- Administración de Usuarios.
- Ficheros temporales.
- Separación de los recursos de desarrollo y producción.
- Gestión de Soportes y Documentos.
- Desechado y reutilización de soportes.
- Almacenamiento de ficheros no automatizados.
- Custodia de soportes.
- Criterios de archivo.
- Seguridad en redes de comunicación.
- Copias de respaldo.
- Régimen de trabajo fuera de los locales de la ubicación del fichero.
- Traslado de documentación.

Este tipo de medidas tiene una doble función. Por un lado serán fundamentales para acreditar que se han asegurado razonablemente los datos de carácter personal en caso de que exista una incidencia. Por el otro, y muy importante también, permiten minimizar el impacto y recuperar el correcto funcionamiento del sistema ante una incidencia real.

Las medidas de seguridad deberán ser la consecuencia de un análisis de riesgos previo que determine las medidas de seguridad adecuadas. El resultado del análisis de riesgos podrá recomendar las mismas medidas que antes, recomendar nuevas medidas o suprimir algunas innecesarias. !

8.6. Notificación de violaciones de seguridad de los datos

Cuando se produzca una violación de la seguridad de los datos personales, el RT deberá notificarla a la autoridad de control competente. La notificación se realizará "sin dilación indebida" y, de ser posible, dentro de las 72 horas después de que haya tenido constancia de ella. No será necesario notificar la violación cuando sea improbable que dicha violación constituya un riesgo para los derechos y las libertades de las personas físicas (art. 33 RGPD). Independientemente de la obligación de notificar, el RT tiene obligación de documentar cualquier quiebra en la seguridad y las medidas correctoras adoptadas.

Se considera que se tiene constancia de una violación de seguridad cuando hay una certeza de que se ha producido y se tiene un conocimiento suficiente de su naturaleza y alcance. 

La mera sospecha de que ha existido una quiebra o la constatación de que ha sucedido algún tipo de incidente sin que se conozcan mínimamente sus circunstancias no deberían dar lugar, todavía, a la notificación, dado que en esas condiciones no sería posible, en la mayoría de los casos, determinar hasta qué punto puede existir un riesgo para los derechos y libertades de los interesados.


Ejemplo: un blog con un hosting situado en EEUU.

los comentarios (que se almacenan en la base de datos de WordPress) serían una transferencia internacional de datos a EEUU, porque se envían y almacenan en un servidor en EEUU. Por la misma lógica, si tu hosting es español, no lo son.

Puede haber casos en que la notificación no pueda realizarse en el plazo máximo de las 72 horas(*). En tal caso cuando se notifique la violación de seguridad deberá expresarse los motivos de la dilación. En el caso en que no sea posible dar toda esta información en el momento de la notificación, el RGPD faculta a que se pueda dar de manera gradual.

por ejemplo, por la complejidad en determinar completamente su alcance.

Además, si la violación de seguridad puede comportar alto riesgo para los derechos de los interesados, el RT deberá comunicarlo sin dilación indebida al interesado (art. 34 RGPD).

Se entiende como violaciones de seguridad o brecha de seguridad todo incidente que origine la destrucción, pérdida o modificación, ya sea de forma accidental o ilícita, de datos personales, o la comunicación o acceso no autorizado a dichos datos. 

La notificación debe incluir un contenido mínimo:

- la naturaleza de la violación de seguridad y las categorías de datos y el número de interesados afectados,
- los datos del delegado de protección de datos (DPD), en su caso;
- descripción de las posibles consecuencias de la violación;
- descripción de las medidas adoptadas o propuestas para remediar la violación y mitigar las consecuencias.

La obligación de notificar las violaciones de seguridad es uno de los aspectos más controvertidos del RGPD, pues plantea muchas cuestiones que el RGPD deja sin resolver:

- ¿cómo debemos entender el concepto de "sin dilación indebida"?
- ¿en qué casos la notificación no es necesaria?
- ¿cuándo es probable que una violación de seguridad puede "comportar alto riesgo"?
- ¿en qué casos y cómo se deberá informar al interesado?
- ¿Qué elementos deberá contener la notificación?

La notificación a los interesados no será necesaria cuando:

- El responsable hubiera tomado medidas técnicas u organizativas apropiadas con anterioridad a la violación de seguridad, en particular las medidas que hagan ininteligibles los datos para terceros, como sería el cifrado.
- Cuando el responsable haya tomado con posterioridad a la quiebra medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice.
- Cuando la notificación suponga un esfuerzo desproporcionado, debiendo en estos casos sustituirse por medidas alternativas como puede ser una comunicación pública.

Documentación adicional

Guidelines on Personal data breach notification under Regulation 2016/679
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

(wp250rev.01) del WP ART.29
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Guía-brechas-seguridad-AEPD
<https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf>

9. Códigos de conducta y certificaciones.

De acuerdo con el RGPD, toda empresa u organización es responsable del cumplimiento de todos los principios de protección de datos, así como de demostrar dicho cumplimiento. El RGPD proporciona herramientas a las empresas u organizaciones para que puedan demostrar su responsabilidad. Así pues los responsables del tratamiento pueden optar por utilizar herramientas como el delegado de protección de datos y complementarlo con códigos de conducta y mecanismos de certificación para demostrar el cumplimiento de los principios de protección de datos.

Tanto el código de conducta como la certificación son instrumentos voluntarios y, por tanto, depende de la organización decidir si adopta un determinado código de conducta o si solicita una certificación.

El RGPD anima a los EM y a las autoridades de control a promover la elaboración de códigos de conducta como forma de contribuir a la correcta aplicación del Reglamento (art.40 RGPD).

9.1. Códigos de conducta

Los códigos de conducta constituyen una muestra de lo que se denomina autorregulación, es decir, la capacidad de las entidades, instituciones y organizaciones para regularse a sí mismas a partir de la normativa establecida. Se podrán elaborar por las asociaciones y otros organismos representativos de categorías de responsables y encargados, para los que serán vinculantes una vez adheridos a los códigos de conducta.

Tienen por objeto especificar la aplicación de las obligaciones que establece el RGPD, en particular respecto a los principios relativos al tratamiento, la legitimidad del mismo, la información que se deberá facilitar a los interesados, el ejercicio de los derechos de los interesados, las medidas de seguridad aplicables, etc. (art. 40.2 RGPD). El mismo código deberá establecer los mecanismos de control de su cumplimiento por parte de los RT que se hayan comprometido a aplicarlo, sin perjuicio de la facultad de supervisión que posee la autoridad competente o la atribuida a un organismo acreditado (art.41 RGPD). Constituyen una herramienta útil para demostrar la adecuación de la organización adherida a las obligaciones que el RGPD le impone.

Ya estaban contemplados en la LOPD. Se llamaban códigos tipo de diferentes sectores como el sanitario o asegurador.

Los códigos de conducta especificarán la aplicación del Reglamento a las características y necesidades de los distintos sectores de actividad en lo que respecta a:

- a)** el tratamiento leal y transparente;
- b)** los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;
- c)** la recogida de datos personales;
- d)** la seudonimización de datos personales;
- e)** la información proporcionada al público y a los interesados;
- f)** el ejercicio de los derechos de los interesados;
- g)** la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;
- h)** las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;
- i)** la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;
- j)** la transferencia de datos personales a terceros países u organizaciones internacionales, o
- k)** los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79 del Reglamento de Protección de Datos Personales.

Cuando una asociación u organismo representativo de un sector o grupo de responsables de tratamiento se disponga a crear un código de conducta (o a modificarlo) presentarán un proyecto a la autoridad de control competente. Después de comprobar la adecuación del mismo a la normativa, la autoridad de control emitirá un dictamen sobre la conformidad del código con el RGPD y lo aprobará si considera que ofrece suficientes garantías. Si el código es aprobado se procederá a su registro y publicación. Un código de conducta puede ser validado en toda la Unión Europea a través de un acto de ejecución de la Comisión. El Comité archivará en un registro todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.

¿Por qué Entidades de certificación? Porque la persona responsable de los datos debe tener sus conocimientos 'validados'



Esquema de las entidades de certificación

Los códigos de conducta y las certificaciones constituyen instrumentos que facilitan poder demostrar que se cumplen con el RGPD, particularmente en relación a la identificación y evaluación del riesgo que supone el tratamiento, y la adopción de buenas prácticas para mitigar el riesgo identificado. Además permiten evaluar rápidamente el nivel de protección de una empresa. !

9.2. Certificaciones

De la misma manera que los códigos de conducta, las certificaciones, los sellos y las marcas de protección de datos facilitan poder demostrar que el responsable o encargado de tratamiento cumple con el RGPD. Sin embargo, tener una certificación no limita la responsabilidad del RT o del ET (art.42.4 RGPD), pero facilita poder probar el cumplimiento normativa, además que la certificación contribuye a aumentar la transparencia, ya que el interesado puede evaluar de manera rápida y eficaz el nivel de protección que ofrece el RT o ET.

La certificación es voluntaria (art. 42.3 RGPD) y sólo podrá ser expedida por un organismo de certificación autorizado (art. 43 RGPD) o por la autoridad de control competente en base a los criterios que aprueben las autoridades o el Comité europeo de protección de datos.

Una organización puede adoptar un mecanismo de certificación aplicado por uno de los organismos de certificación que haya recibido la acreditación de una APD o un organismo de acreditación nacional o ambos, según establezca la legislación de cada Estado miembro. !

10. Transferencias Internacionales de Datos.

Este concepto es muy relevante en protección de datos en un contexto de sociedad digital globalizada en donde, de forma habitual, utilizamos herramientas que almacenan datos personales que están ubicadas en países fuera de la Unión Europea. Es el caso de herramientas como email marketing, analíticas o incluso redes sociales.

Se entiende como transferencia internacional de datos (TID), la transmisión de datos personales desde el Espacio Económico Europeo (EEE), es decir, los países de la UE más Liechtenstein, Islandia y Noruega a otros países fuera de la Unión europea.

Por ejemplo: si tienes un simple blog con un hosting situ en EEUU, los comentarios (que se almacenan en la base de datos de WordPress) serían una transferencia internacional de datos a EEUU, porque se envían y almacenan en un servidor en EEUU. Por la misma lógica, si tu hosting es español, no lo son.

Ejemplo: un blog con un hosting situado en EEUU.

los comentarios (que se almacenan en la base de datos de WordPress) serían una transferencia internacional de datos a EEUU, porque se envían y almacenan en un servidor en EEUU. Por la misma lógica, si tu hosting es español, no lo son.

Una de las novedades que introduce el Reglamento respecto a la regulación anterior de las TID es la posibilidad de que el encargado de tratamiento pueda realizar TID. Trasferir datos personales desde un país de la UE a un país fuera del EEE sólo es posible cuando:

1. Existe una decisión de adecuación.
2. No habiendo decisión de adecuación, se ofrecen garantías adecuadas.

10.1. El sistema de decisiones de adecuación

La Comisión Europea mantiene una lista de países, territorios, un sector específico de un país o una organización internacional fuera del EEE que ofrecen un nivel adecuado de protección para los datos personales (art.42). En tal caso las transferencias de datos no requerirán autorización específica de la AEPD. El RGPD introduce la obligación de revisar de manera periódica, al menos cada cuatro años, la decisión de adecuación por parte de la Comisión.

Para consultar los países que ofrecen un nivel adecuado de protección podéis consultarlo aquí

https://ec.europa.eu/info/law/law-topic/data-protection_en

10.2. Privacy shield.

Este *Escudo de Privacidad* es un acuerdo entre las autoridades de EE.UU. y las europeas, donde se establece una colaboración mutua y están obligadas a publicar normas específicas sobre el tratamiento de los datos que recopilan. Esto también implica que los gobiernos de los Estados implicado no podrán acceder de forma indiscriminada a los datos, sólo lo harán cuando sea imprescindible y contando con las debidas garantías.

El EU-US Privacy Shield fue adoptado en julio de 2016 por la Comisión Europea mediante la Decisión (UE) 2016/1250 de 12 de julio de 2016.

Para saber más sobre el Privacy Shield consultar Guide to the EU-US Privacy Shield

https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pdf

10.3. Normas corporativas vinculantes (Binding Corporate Rules).

La BCRs son un conjunto de reglas o cláusulas corporativas vinculantes que tienen por objeto establecer las prácticas que una entidad lleva a cabo en materia de tratamiento de datos de carácter personal con la finalidad de facilitar las transferencias internacionales de datos en el seno de dicha corporación. Las BCRs constituyen un instrumento que los grupos multinacionales pueden hacer valer ante las autoridades de protección de datos, para garantizar la legalidad de las operaciones de transferencia de datos en su organización, independientemente de que el país de destino garantice o no un “adecuado nivel de protección” conforme a la normativa vigente en el país de origen de los datos (artículo 41). Éstas deben de tener un contenido mínimo y ser aprobadas por la autoridad de control competente (AEPD).

Dichas normas corporativas vinculantes únicamente facultan para las TID dentro del mismo grupo de empresas, pero en ningún caso facultan para realizar TID fuera del grupo.

Para consultar la lista de empresas europeas que han optado por este sistema.

https://ec.europa.eu/info/law/law-topic/data-protection_en

10.4. Excepciones.

Se prevé la posibilidad de realizar transferencias en determinadas circunstancias sin necesidad de aportar garantías adecuadas (art 43). La relación de excepciones recoge varios supuestos, especificados artículo 49.1 del Reglamento (UE) 2016/679.

- a) el interesado ha dado consentimiento explícito después de que haya sido informado de los riesgos para él de la TID.
- b) la TID sea necesaria para la ejecución de un contrato entre el interesado el RT o para la ejecución de medidas contractuales solicitadas por el propio interesado;
- c) la TID sea necesaria para la ejecución la celebración o la ejecución de un contrato en interés del interesado, entre el RT y un tercero;

- d) por razones de interés público, para el ejercicio o la defensa de reclamaciones;
- e) para proteger los intereses vitales del interesado cuando este se encuentre incapacitado para dar su consentimiento;
- f) cuando se acredite un interés legítimo y la TID se realice desde un registro público que esté abierto a consulta del público en general, en este no abarcará la totalidad de los datos que se encuentren en el registro.

A pesar de que no se pudiera cumplir ninguno de los supuestos mencionados, todavía sería posible un supuesto concreto en que el RT podría realizar una TID. En efecto, el RGPD introduce una novedad respecto a la normativa anterior, la posibilidad de realizar una TID basada en el interés legítimo imperioso perseguido por el RT. Para que sea posible la TID no deberá ser repetitiva, deberá afectar solo a un número limitado de interesados, ser necesaria para conseguir los intereses legítimos imperiosos del RT y no deberán prevalecer los derechos y libertades del interesado. El RT deberá aportar garantías adecuadas después de evaluar todas las circunstancias concurrentes. Si se cumplen todas estas condiciones el RT informará a la autoridad de control (AEPD) de la TID y a los interesados facilitándoles toda la información preceptiva y informándoles de los intereses legítimos imperiosos perseguidos (art. 47.1 segundo RGPD).

Más información en
EDPB_Guidelines

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2018_derogations_en.pdf

11. Las Autoridades de Control y el régimen sancionador

11.1. Las Autoridades de Control.

Cada EM deberá establecer autoridades de control (AC) capacitadas para desempeñar sus funciones y ejercer sus competencias con independencia. En función de la estructura constitucional, organizativa y administrativa, los EM podrán tener una o más AC. En virtud de lo anterior, hasta la fecha en el Estado Español se han creado tres AC: la Agencia Española de Protección de Datos (AEPD)(1); la Autoridad Catalana de Protección de Datos (APDCAT)(2) y la Agencia Vasca de Protección de Datos (AVPD)(3). Cada AC es competente en el territorio del EM para ejercer los poderes y desempeñar las funciones que el Reglamento les confiere. En el Estado Español las AC autonómicas son competentes para ejercer sus poderes y funciones en el ámbito del territorio de la Comunidad Autónoma, limitada al ámbito de sus competencias. En cambio, la AEPD ejerce sus poderes y funciones en todo el territorio del Estado respecto a los tratamientos realizados por las AAPP del Estado (también en el resto de Autonomías que no han desplegado competencias en la materia), y otros organismos públicos y privados, así como de particulares y empresas.

Todas la AC deberán estar dotadas de los recursos financieros y humanos necesarios para realizar sus funciones con eficacia. Los miembros de las AC deberán ser nombrados mediante procedimientos transparentes por el Parlamento, el Gobierno o el Jefe del EM. En el caso de la AEPD es el Gobierno Español quien designa al director/a de la Agencia mediante decreto.

Las AC ejercen funciones de supervisión, asesoramiento, consultivas, de sensibilización de los ciudadanos, etc. (Art.57 RGPD)

Para poder ejercer sus funciones las AC están dotadas de poderes (art. 58 RGPD):

- de investigación: por ejemplo, ordenar al RT o ET que le faciliten la información requerida.
- correctivos: sancionar con una advertencia o con un apercibimiento la posibilidad de infracción o la infracción del Reglamento, etc.;
- de autorización y consultivos: aprobar normas corporativas vinculantes, emitir dictámenes sobre asuntos relacionados con la protección de datos, etc.

(1)
<https://www.aepd.es/>

(2)
<http://apdcatt.gencat.cat/es/inici/>

(3)
<http://www.avpd.euskadi.eus/s04-5213/es>

11.2. El Régimen sancionador

artículos 77 a 84 GDPR


El RGPD establece un régimen sancionador flexible. Junto a las sanciones económicas, el RGPD también contempla la aplicación otras acciones correctivas (art. 83 RGPD).

- Las sanciones económicas deben ser efectivas, proporcionadas y disuasorias, pudiendo llegar hasta un máximo de 20.000.000 EUR o, tratándose de una empresa, a la cuantía equivalente al 4% del volumen de negocio anual de la empresa (lo que sea mayor). A priori son cifras astronómicas, si bien, el Reglamento ofrece diferentes criterios de modulación.
- Las acciones correctivas incluyen advertencias, apercibimientos, órdenes de adaptación de tratamientos, limitaciones temporales o definitivas de tratamientos, incluida la prohibición, etc.

Las multas administrativas (sanciones) se impondrán, en función de las circunstancias de cada caso individual y serán efectivas, proporcionadas y disuasorias. Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente un conjunto de aspectos definidos en el artículo 83 del RGPD. El rango de sanciones según su importancia es ahora:

- Sanciones Leves: No se establece un rango mínimo de cuantía
- Sanciones graves: Multa administrativa de hasta 10.000.000€ o, en el caso de empresas, de cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, lo que resulte mayor en cuantía.
- Sanciones muy graves: Multa administrativa de hasta 20.000.000€ o, en el caso de empresas, de cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, lo que resulte mayor en cuantía.

Cualquier Interesado que haya sufrido un perjuicio, material o inmaterial, como consecuencia de una operación de tratamiento que no se atenga a la normativa de protección de datos, tiene la potestad de presentar una reclamación ante la Autoridad de Control correspondiente y puede requerir una indemnización si se demuestra que sus derechos se han visto vulnerados. El interesado ahora tiene derecho a reclamar, a tutela judicial y a indemnización.

El incumplimiento por parte de una organización puede conllevar sanciones, indemnizaciones y otras acciones correctivas a la vez. 

Resumen

“La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental (...)”.

Considerando 1 GDPR

Las nuevas tecnologías de transmisión y de tratamiento de información han conllevado una elevada dispersión de los datos personales. Además, la diversidad de información que puede ser asociada a una persona es amplia. Los datos considerados como personales son utilizados para muchas actividades cotidianas. Por ello los estados, cada vez más conscientes de la situación, buscan regular (con leyes) las diferentes situaciones en que los datos deben ser protegidos. Ante un mundo globalizado, estas normas ya no pueden ser solamente de carácter nacional, sino que deben trascender las fronteras.

Así pues, el reglamento general de protección de datos es una normativa a nivel de la Unión Europea, por lo que cualquier empresa de la unión, o aquellas empresas que tengan negocios en la Unión Europea, que manejen información personal de cualquier tipo tienen la obligación de adoptar aquellas medidas que aseguren razonablemente que, a priori, están en condiciones de cumplir con los principios, garantías y derechos establecidos en el Reglamento.

El fundamento de este reglamento es **asegurar y acreditar la protección de los datos**. Por ello, además del cumplimiento, la organización debe estar en condiciones de demostrar las medidas de seguridad aplicadas si llegara el caso y **acreditar** que se cumple el Reglamento. El objetivo es evitar así los riesgos de diversa probabilidad y gravedad para los derechos fundamentales de los usuarios.

En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar la forma en que aplicarán las medidas que el GDPR prevé, asegurándose de que esas medidas son las más adecuadas y que pueden demostrarlo ante los interesados y las autoridades ante una supervisión. El objetivo es evitar a los titulares de los datos unos daños que a posteriori pueden ser muy difíciles o imposibles de reparar.

En síntesis, lo que el GDPR exige es una **actitud consciente, diligente y pro-activa** del tratamiento de los datos que se lleven a cabo.

Existe un importante cambio con respecto a la ley anterior (Ley Orgánica de Protección de Datos, LOPD) que buscaba evitar la infracción de los derechos

de los interesados como obligación principal. El GDPR trata de anticiparse a la infracción o lesión de derechos, aunque también establece importantes sanciones cuando no se cumpla con la normativa.

Lo que es evidente es que el ciudadano es cada vez más consciente de sus datos y los derechos asociados y cada vez será más exigente con las empresas y profesionales que los gestionan.

Glosario

AC: Autoridad de control

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

AEPD: Agencia Española de Protección de Datos

Afectado o interesado o titular de los datos: Persona física titular de los datos que sean objeto de tratamiento. Tal y como detalla el nuevo reglamento, el afectado dispone de una serie de derechos como el derecho a la información sobre la identidad del responsable de los datos y los fines del tratamiento, entre otros.

Autoridad de control: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51; 4.5.2016 L 119/34 Diario Oficial de la Unión Europea ES

Brecha de seguridad. Véase violación de la seguridad de los datos personales.

Categorías especiales de datos: datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, los 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 orientaciones sexuales (artículo 9 de la Ley).

Consentimiento del interesado: Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

Copia de respaldo o Backup: Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Datos biométricos: Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos. El RGPD aclara que el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales. Única-

mente se considerarán datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.

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

Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de esa persona.

Datos personales: Toda información sobre una persona física identificada o identificable («el interesado»). Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona

Datos relativos a la salud. Datos relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud. Entre otros: la información recogida en la inscripción a efectos de la prestación de asistencia sanitaria, la recogida con prestación de tal asistencia; todo número, símbolo o dato asignado a una persona que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes, incluida la procedente de datos genéticos y muestras biológicas; y cualquier información relativa a una enfermedad, discapacidad, riesgo de padecer enfermedades; el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente.

Destinatario: Persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen los datos, se trate o no de un tercero. No obstante, no se consideraran destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de acuerdo con el Derecho de la UE o de los EM.

Elaboración de perfiles: Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

EM: Estado miembro

Encargado de tratamiento: persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos por cuenta del responsable del tratamiento.

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

Fichero: Conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

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

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

Interesado: véase Afectado o interesado o titular de los datos

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Limitación del Tratamiento: Marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

Normas corporativas vinculantes: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

Persona identificable: Toda persona cuya identidad pueda determinarse directa o indirectamente mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social.

REGLAMENTO: (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos. Los términos reglamento, GDPR, DRGP, Reglamento (UE)

2016/679 del Parlamento Europeo o nuevo reglamento de protección de datos hacen referencia a lo mismo, el texto del reglamento puede consultarse en:

<https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES>

Responsable de tratamiento: persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

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

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

Seudonimización: El tratamiento de datos personales de manera que ya no puedan atribuirse al interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

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

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

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

Titular de los datos: véase Afectado o interesado o titular de los datos.

Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización estructuración o conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación supresión o destrucción.

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

Violación de la seguridad de los datos personales: Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;