MADRID

LEY DE PROTECCIÓN DE DATOS PARA ENTIDADES Y COLECTIVOS CIUDADANOS

Autor: Sergio Rojas del Saz

Fundacion Gestión y Participación Social

LEY DE PROTECCIÓN DE DATOS PARA ENTIDADES Y COLECTIVOS CIUDADANOS

Fundación Gestión y Participación Social

Elaborado por: Fundación Gestión y Participación Social

Autor: Sergio Rojas del Saz

INDICE

MARCO JURÍDICO

A partir del 25 de mayo de 2018 ya es aplicable el nuevo Reglamento General de Protección de Datos (RGPD):

> *REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.*

Este reglamento es una norma directamente aplicable y no requiere de trasposición ni desarrollo en cada uno de los países de la Unión. De aquí en adelante nos referiremos a él como RGPD

En España, después de un tiempo de convivencia del reglamento europeo con la antigua Ley Orgánica en materia de Protección de Datos, en diciembre de 2018 se aprobó la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Esta Ley Orgánica prácticamente viene a trasladar lo ya regulado por RGPD cerrando cualquier especulación existente respecto a preceptos aún en vigor de la Ley Orgánica de 1999.

Por lo tanto, en este curso nos centraremos principalmente en el Reglamento Comunitario RGPD y en la Ley Orgánica 3/2018

Antes de entrar en desarrollo de la normativa, conviene analizar brevemente el marco constitucional que fundamenta la Protección de Datos. El objetivo de esta normativa es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

La CARTA DE LOS DERECHOS FUNDAMENTALES DE LA U.E. (Estrasburgo de 12 de diciembre de 2007) establece en su artículo 8 que:

Artículo 8 Protección de datos de carácter personal

1. *Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*
2. *Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.*
3. *El respeto de estas normas estará sujeto al control de una autoridad independiente.*

A su vez, el artículo 18 de la Constitución Española establece que:

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

…

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

Como podemos observar, la carta de Derechos Fundamentales de la Unión Europea es más específica con la protección de los datos de Carácter Personal, un texto sin duda más adaptado a los tiempos actuales, si bien, la carta magna española ya preveía la necesidad de garantizar la intimidad personal y familiar.

Por lo tanto, lo primero que se debe de tener en cuenta es que esta regulación no hace más que garantizar la protección de un derecho fundamental de los ciudadanos y ciudadanas europeos.

Aspectos elementales de la norma

PROTECCIÓN DE DERECHOS FUNDAMENTALES: Se establecen las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos, con el objetivo de proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

Es importante destacar que, igual que se protegen los datos, también se protege la libre circulación de los mismos en la Unión. Por lo que la circulación de los datos no podrá ser restringida ni prohibida.

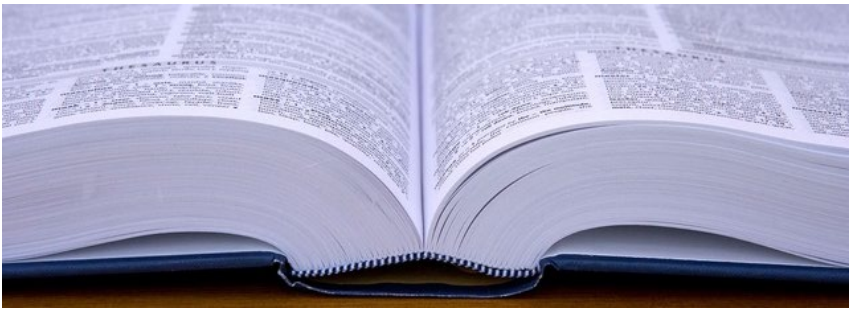
AMBITO DE APLICACIÓN: Se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales (manual). La norma busca que pueda ser aplicada de forma tecnológicamente neutra que no dependa de las técnicas utilizadas. Así se garantiza su perdurabilidad en el tiempo independientemente de las posibles tecnologías futuras que se utilicen en el tratamiento de los datos.

No obstante, debe tenerse en cuenta que no se aplica el reglamento en aquellos tratamientos efectuados por una persona

física en el ejercicio de actividades exclusivamente personales o domésticas, incluida la correspondencia, agendas de direcciones y la actividad en redes sociales.

Tampoco se aplicará el reglamento cuando el tratamiento de datos sea llevado a cabo por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

ÁMBITO TERRITORIAL DEL RGPD. Se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.



DEFINICIONES

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;

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

LIMITACIÓN DEL TRATAMIENTO: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

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;

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

FICHERO: conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

RESPONSABLE DEL TRATAMIENTO: 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;

ENCARGADO DEL TRATAMIENTO: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

DESTINATARIO: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades

públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

TERCERO: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

CONSENTIMIENTO DEL INTERESADO: 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;

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;

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

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 personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

PRINCIPIOS RELATIVOS AL TRATAMIENTO

Se establece lo que se ha venido en llamar el **Principio de Responsabilidad Proactiva**. Este Principio va a ser muy importante a partir de ahora, y viene a significar la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la Ley Orgánica y el RGPD.

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 adecuadas para cumplir con la normativa y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.

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.

Los principios que se deberán tener en cuenta a la hora del tratamiento de datos de carácter personal son:

a) LICITUD, LEALTAD Y TRANSPARENCIA: Los datos personales deberán ser tratados de manera lícita, leal y transparente en relación con el interesado;

b) LIMITACIÓN DE LA FINALIDAD: Los datos personales deberán ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. 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;

c) MINIMIZACIÓN DE DATOS: Los datos personales deberán ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados;

d) EXACTITUD: Los datos personales deberán 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;

e) LIMITACIÓN DEL PLAZO DE CONSERVACIÓN: Los datos personales deberán ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas a fin de proteger los derechos y libertades del interesado

f) INTEGRIDAD Y CONFIDENCIALIDAD: Los datos personales deberán ser 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.

Y como decíamos en relación a la Responsabilidad Proactiva, se establece que: **El responsable del tratamiento será responsable del cumplimiento de estos principios y, muy importante, deberá ser capaz de demostrarlo**.

TRATAMIENTO LÍCITO Y CONSENTIMIENTO

Como hemos visto en el apartado anterior, uno de los principios elementales de la protección de datos es garantizar que el tratamiento que se haga de los mismos se haga de manera transparente, leal y lícita. Además, el responsable del tratamiento tiene que estar en disposición de demostrar que ha sido así. Por tanto, es muy importante conocer cuándo se considera que un tratamiento es lícito. Para ello, deberá cumplirse al menos una de las siguientes condiciones establecidas en el RGPD:

a) El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Esto no será de aplicación si es realizado por las autoridades públicas en el ejercicio de sus funciones

Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que no cumpla esta condición.

El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Consentimiento de menores

En relación al consentimiento dado por menores a una oferta directa de servicios de la sociedad de la información, **el tratamiento de los datos personales de un menor legitimado en el consentimiento se considerará lícito cuando tenga como mínimo 14 años**. Si es menor de 14 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el menor, teniendo en cuenta la tecnología disponible.

CATEGORÍAS ESPECIALES DE DATOS PERSONALES

Quedan prohibidos el tratamiento de datos personales que revelen el **origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical**, y el tratamiento de **datos genéticos, datos biométricos** dirigidos a identificar de manera unívoca a una persona física, datos relativos a la **salud** o datos relativos a la **vida sexual o la orientación sexual** de una persona física.

Solamente podrán tratarse este tipo de datos cuando concurra una de las circunstancias siguientes:

a) **el interesado dio su consentimiento explícito** para el tratamiento de dichos datos personales con los fines especificados. En el caso de la ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico, aun existiendo el consentimiento del interesado, no será lícito el tratamiento de datos salvo que concurra alguna otra circunstancia de las expuestas a continuación:

b) el tratamiento es necesario para el **cumplimiento de obligaciones** y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del **Derecho laboral y de la seguridad y protección social**, en la

medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario **para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado**, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, **por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro**, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que **el interesado ha hecho manifiestamente públicos**;

f) el tratamiento es necesario para la formulación, el ejercicio o la **defensa de reclamaciones** o cuando los tribunales actúen en ejercicio de su **función judicial**;

g) el tratamiento es necesario por razones de un **interés público esencial**, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de **medicina preventiva o laboral**, evaluación de la capacidad laboral del

trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario;

i) el tratamiento es necesario por razones de **interés público en el ámbito de la salud pública**, como la protección frente a **amenazas transfronterizas** graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con **fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos**, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Resumen de datos especialmente protegidos:

- Origen étnico o racial.
- Opiniones políticas.
- Convicciones religiosas o filosóficas.
- Afiliación sindical.
- Datos de salud, genéticos o biométricos.
- Datos de salud.
- Vida sexual y orientación sexual.

DERECHOS DE LOS INTERESADOS

Con carácter general, los responsables deben facilitar a los interesados el ejercicio de sus derechos, y los procedimientos y las formas para ello deben ser visibles, accesibles y sencillos.

- Se requiere que los responsables posibiliten la presentación de solicitudes por medios electrónicos, especialmente cuando el tratamiento se realiza por estos medios. Además, debe poderse acreditar el procedimiento.
- Los responsables deberán tomar medidas para verificar la identidad de quienes soliciten acceso y de quienes ejerzan los derechos.
- El ejercicio de los derechos será gratuito para el interesado, excepto en los casos en que se formulen solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas, el responsable podrá cobrar un canon que compense los costes administrativos de atender a la petición o negarse a actuar (el canon no podrá implicar un ingreso adicional para el responsable, sino que deberá corresponderse efectivamente con el verdadero coste de la tramitación de la solicitud).

- Si el responsable decide no atender una solicitud, deberá informar de ello, motivando su negativa, dentro del plazo de un mes desde su presentación.
- El responsable deberá informar al interesado sobre las actuaciones derivadas de su petición en el plazo de un mes (podrá extenderse dos meses más cuando se trate de solicitudes especialmente complejas y deberá notificar esta ampliación dentro del primer mes)
- El responsable que trate una gran cantidad de información sobre un interesado podrá pedir a éste que especifique la información a que se refiere su solicitud de acceso.
- El responsable podrá contar con la colaboración de los encargados para atender al ejercicio de derechos de los interesados, pudiendo incluir esta colaboración en el contrato de encargo de tratamiento.

Derecho de información

Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en un interés legítimo del responsable o un tercero, se deberá informar de los mismos;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional

Además, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

g) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

h) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

i) cuando el tratamiento esté basado en el consentimiento del interesado, la existencia del derecho a retirar dicho consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

j) el derecho a presentar una reclamación ante una autoridad de control (Agencia Española de Protección de Datos);

k) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

l) la existencia de decisiones automatizadas, incluida la elaboración de perfiles.

Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente.

Todo ello no será aplicable cuando y en la medida en que el interesado ya disponga de la información.

Derecho de acceso

El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales (fines, categorías de datos, destinatarios de los datos, plazo previsto de conservación, etc.)

El interesado tiene el derecho a obtener copia de los datos siempre que no afecte negativamente a los derechos y libertades de otros.

Derecho de rectificación

El interesado tendrá derecho a la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional

Derecho de supresión (el derecho al olvido)

El interesado tendrá derecho a la supresión de los datos personales que le conciernan, el responsable estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento

c) el interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal;

Cuando el responsable haya hecho públicos los datos personales y esté obligado a suprimir dichos datos, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

No se aplicará la supresión cuando el tratamiento sea necesario

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos,

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Derecho a la limitación del tratamiento

El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Cuando el tratamiento de datos personales se haya limitado, sólo podrán ser objeto de tratamiento con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público.

Todo interesado que haya obtenido la limitación del tratamiento será informado por el responsable antes del levantamiento de dicha limitación.

Derecho a la portabilidad de los datos

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo

impida el responsable al que se los hubiera facilitado, cuando el tratamiento esté basado en el consentimiento y cuando el tratamiento se efectúe por medios automatizados y no afecte negativamente a los derechos y libertades de otros.

El interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

Este derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Derecho de oposición

El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

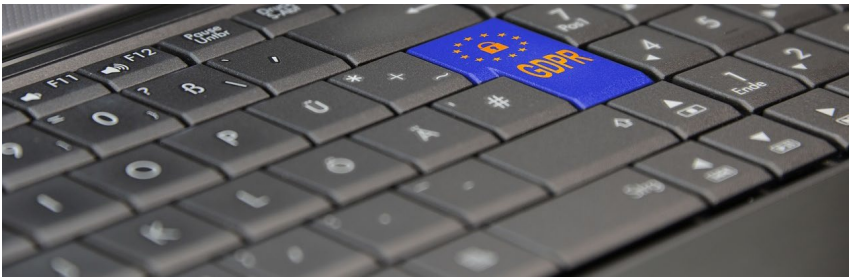
Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

En el contexto de la utilización de servicios de la sociedad de la información el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Obligación de notificación

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.



MEDIDAS DE RESPONSABILIDAD ACTIVA

Se establecen una serie de 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. Brevemente mencionamos algunas de estas medidas.

Análisis de riesgo

El RGPD condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados. Determinadas medidas solo deberán aplicarse cuando el tratamiento suponga un alto riesgo para los derechos y libertados (por ejemplo, Evaluaciones de impacto sobre la Protección de Datos). Otras medidas deberán modularse en función del nivel y tipo de riesgo que el tratamiento conlleve.

Todos los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo.

Grandes organizaciones utilizarán metodologías de análisis de riesgo existentes más complejas. Sin embargo, las organizaciones de menor tamaño y con tratamientos de poca complejidad, realizarán análisis a través de una reflexión, mínimamente

documentada, sobre las implicaciones de los tratamientos en los derechos y libertades de los interesados.

La reflexión deberá dar respuesta a cuestiones como las que se exponen a continuación. Cuanto mayor sea el número de respuestas afirmativas mayor sería el riesgo que podría derivarse del tratamiento. Si la respuesta a estas preguntas y otras del mismo tipo fuera negativa, es razonable concluir que la organización no realiza tratamientos que generen un elevado nivel de riesgo y que, por tanto, no debe poner en marcha las medidas previstas para esos casos.

- ¿Se tratan datos sensibles?
- ¿Se incluyen datos de una gran cantidad de personas?
- ¿Incluye el tratamiento la elaboración de perfiles?
- ¿Se cruzan los datos obtenidos de los interesados con otros disponibles en otras fuentes?
- ¿Se pretende utilizar los datos obtenidos para una finalidad para otro tipo de finalidades?
- ¿Se están tratando grandes cantidades de datos, incluido con técnicas de análisis masivo tipo big data?
- ¿Se utilizan tecnologías especialmente invasivas para la privacidad, como las relativas a geolocalización, videovigilancia a gran escala o ciertas aplicaciones del Internet de las Cosas?

La Agencia Española de Protección de Datos, facilitará herramientas que permitan realizar este análisis de riesgos.

Registro de actividades de tratamiento

Los responsables y encargados deberán mantener un registro de operaciones de tratamiento en el que se contenga la información que establece la normativa y que contenga cuestiones como:

- Nombre y datos de contacto del responsable y del Delegado Protección de Datos si existiese.
- Finalidades del tratamiento.
- Descripción de categorías de interesados y de los datos tratados.
- Categorías de destinatarios.
- Transferencias internacionales de datos.
- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Están exentas las organizaciones que empleen a menos de 250 trabajadores, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya **categorías especiales** de datos o datos relativos a condenas e infracciones penales.

Desde el diseño y por defecto

Estas medidas se incluyen dentro de las que debe aplicar el responsable con anterioridad al inicio del tratamiento y también cuando se esté desarrollando.

Este tipo de medidas reflejan muy directamente el enfoque de responsabilidad proactiva. Se trata de pensar en términos de protección de datos desde el mismo momento en que se diseña un tratamiento, un producto o servicio que implica el tratamiento de datos personales.

Desde el inicio, los responsables deben tomar medidas organizativas y técnicas para integrar en los tratamientos garantías que permitan aplicar de forma efectiva los principios de la Protección de Datos.

Los responsables deben adoptar medidas que garanticen que solo se traten los datos necesarios en lo relativo a la cantidad de datos tratados, la extensión del tratamiento, los periodos de conservación y la accesibilidad a los datos.

Medidas de seguridad

La anterior Ley Orgánica de Protección de datos determinaba con detalle y de forma exhaustiva las medidas de seguridad que debían aplicarse según el tipo de datos objeto de tratamiento y estaban basadas casi exclusivamente en el tipo de datos que se trataban.

Sin embargo, con la nueva normativa, los responsables y encargados establecerán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo y tomando en cuenta más variables además del tipo de datos.

Las medidas técnicas y organizativas de seguridad, deberán establecerse teniendo en cuenta:

- El coste de la técnica.
- Los costes de aplicación.
- La naturaleza, el alcance, el contexto y los fines del tratamiento.
- Los riesgos para los derechos y libertades.

Las medidas de seguridad que fijaba el anterior Reglamento de Desarrollo de la LOPD, no son válidas de forma automática. No obstante, en algunos casos los responsables podrán seguir aplicando las mismas medidas que establecía el Reglamento de la LOPD si los resultados del análisis de riesgos previo concluyen que las medidas son realmente las más adecuadas para ofrecer un nivel de seguridad adecuado. En ocasiones será necesario

completarlas con medidas adicionales o prescindir de alguna de las existentes.

Notificación de "violaciones de seguridad de los datos"

El RGPD define las violaciones de seguridad de los datos, más comúnmente conocidas como "quiebras de seguridad", de una forma muy amplia, que incluye todo incidente 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.

Sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad y deben ser notificadas.

Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

La notificación de la quiebra a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.

Los responsables deben documentar todas las violaciones de seguridad.

En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con una notificación dirigida a estos últimos. El objetivo de la notificación a los afectados es permitir que puedan tomar medidas para protegerse de sus consecuencias tan pronto como sea posible.

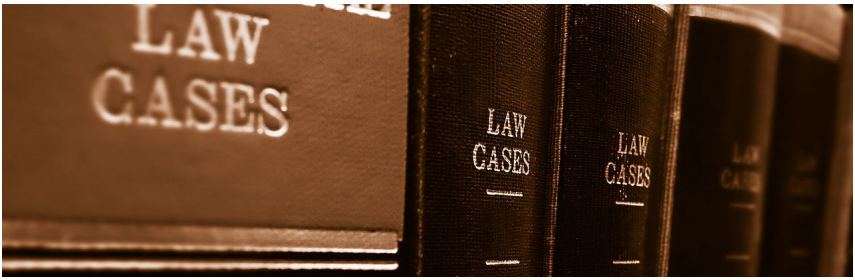
Evaluación de impacto sobre la protección de datos

Los responsables de tratamiento deberán realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados. En particular si utiliza nuevas tecnologías.

Delegado de protección de datos

El RGPD establece la figura del Delegado de Protección de Datos (DPD), que será obligatorio en:

- Autoridades y organismos públicos.
- Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala.
- Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles.



DERECHO A RECLAMACIONES Y SANCIONES

Con la entrada en vigor de la nueva normativa de Protección de datos, se han endurecido considerablemente las sanciones.

Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe la normativa. En España, esta autoridad de control la ejerce la Agencia Española de Protección de Datos.

La autoridad de control ante la que se haya presentado la reclamación informará al reclamante sobre el curso y el resultado de la reclamación.