Máster en Ingeniería Informática
Universidad Complutense de Madrid, 2021-2022

Humberto Martínez Silva

Protección de Datos

https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf

Ley 3/2018

Reglamento General de Protección de Datos (RGPD)

Agencia Española de Protección de Datos (AEPD)

La **Agencia Española de Protección de Datos (AEPD)** es la **autoridad de control independiente** que vela por el cumplimiento de la normativa de protección de datos y garantiza y tutela el derecho fundamental a la protección de datos de carácter personal.

Agencia Española de Protección de Datos (AEPD)

En relación con los afectados

- Atender a sus peticiones y reclamaciones.
- Información de los derechos reconocidos en la Ley.
- Promover campañas de difusión a través de los medios.

En relación con quienes tratan datos

- Emitir autorizaciones previstas en la Ley.
- Requerir **medidas de corrección**.
- Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos.
- Ejercer la **potestad sancionadora**.
- Recabar ayuda e información que precise.
- Autorizar las transferencias internacionales de datos.

Ref: https://ayudaleyprotecciondatos.es/2010/05/03/que-es-la-agencia-espanola-de-proteccion-de-datos-aepd/#Funciones

Agencia Española de Protección de Datos (AEPD)

En materia de telecomunicaciones

•Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente.

Ref: https://ayudaleyprotecciondatos.es/2010/05/03/que-es-la-agencia-espanola-de-proteccion-de-datos-aepd/#Funciones

Normativa fundamental

- (**LOPD**) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- (**RGPD -** Reglamento general de protección de datos) 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.

Ley vs Reglamento

- *La Ley establece principios y regulaciones de carácter general, aplicables a toda persona que caiga en los supuestos en ella previstos.*

- *El Reglamento define la forma en que la Ley se va a llevar a cabo, el cómo hacer, qué hacer, dónde hacerlo, a partir de qué momento, hasta que fecha límite, etc.*

¿Qué es un dato de carácter personal?

Los datos de carácter personal son cualquier información referente a personas físicas identificadas o identificables, pudiendo ser identificable toda persona cuya identidad pueda determinarse mediante un identificador (por ejemplo, un nombre, un número de identificación, datos de localización o un identificador en línea) o mediante el uso de uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de las personas.

¿Qué es un dato de carácter personal?

Dependiendo del tipo de datos que se traten, éstos pueden ser:

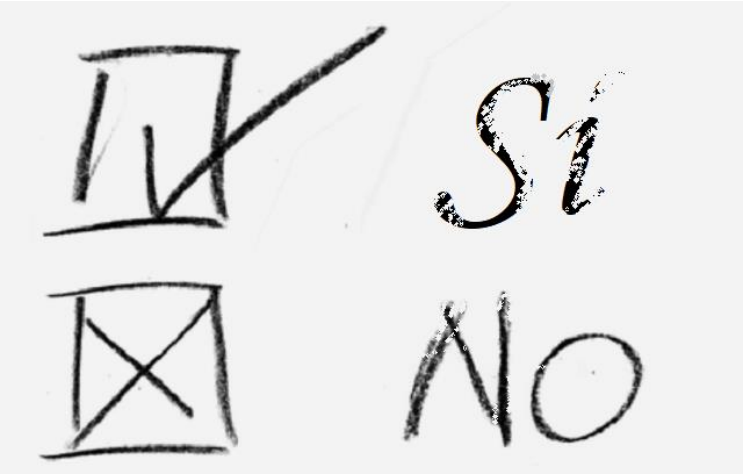
- identificativos (nombre, apellidos, número del documento nacional de identidad).
- referidos a tu situación laboral, financiera o de salud.

Categorías especiales de datos:

- datos de salud.
- origen étnico o racial.
- opiniones políticas.
- convicciones religiosas o filosóficas.
- afiliación sindical.
- datos genéticos.
- datos biométricos.
- vida u orientación sexual.

Consentimiento del afectado

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.



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

Principios de protección de datos

Principio de licitud, lealtad y transparencia.

Principio de exactitud de los datos.

Principio de limitación de la finalidad.

Principio de minimización de datos.

Principio del plazo de conservación.

Principio de integridad y seguridad.

Principios de protección de datos

Cuando se solicite consentimiento durante la formalización de un contrato para finalidades que no tengan relación con el mismo, debe permitirse que se manifieste expresamente la negativa al tratamiento o comunicación de datos.

Tampoco podemos enviar comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica si no se ha solicitado o autorizado expresamente.

El RGPD no permite el denominado “consentimiento tácito”, ya que para prestar el consentimiento se requiere una declaración o una clara acción afirmativa.

Principios de protección de datos

Principio de licitud, lealtad y transparencia: supone que cuando se recaben datos de carácter personal deben ser tratados de manera lícita, leal y transparente.

Ejemplo: no pueden utilizarse datos personales para realizar una contratación fraudulenta, dando un alta en un servicio que no se ha solicitado.

Principios de protección de datos

Principio de Exactitud de los datos: los datos personales serán exactos, adoptándose medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos respecto a los fines para los que se tratan.

Principios de protección de datos

Principio de limitación de la finalidad: los datos personales serán recogidos para unos fines determinados, explícitos y legítimos, y no serán tratados para otros fines.

Ejemplo: si se recaban datos personales "*para ser tratados para mejorar la experiencia en el sistema de todos los usuarios*", esta finalidad no se ajustaría a este principio.

Principios de protección de datos

Principio de minimización de datos: los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No es posible, según este principio, recabar y tratar datos simplemente por si pudieran resultar útiles o "por tenerlos".

Ejemplo: si suscribimos a un servicio de alertas a través del envío de SMS, sería suficiente con facilitar, además del nombre y apellidos, el número de teléfono móvil, no siendo necesario añadir el número de teléfono fijo. Si para una finalidad determinada no es necesario conocer las pautas de navegación de un usuario, **no se podrá hacer ese seguimiento** sin su consentimiento.

Principios de protección de datos

Principio del plazo de conservación: los datos personales serán mantenidos de forma que se permita la identificación de los interesados por un plazo de tiempo no superior al necesario para cumplir con los fines del tratamiento. La conservación de datos debe limitarse a las finalidades para las cuales se han recabado dichos datos. Una vez cumplidas estas finalidades, los datos deben ser borrados o, al menos, desprovistos de todo elemento que permita identificar a los interesados.

Ejemplo: Cuando recaben tus datos de carácter personal el responsable debe informarte sobre el período o criterios de conservación de tus datos personales.

Principios de protección de datos

Principio del plazo de conservación:

No se considera un tratamiento incompatible si tus datos personales se utilizan posteriormente con **fines de archivo en interés público, investigación científica e histórica, así como fines estadísticos**, de manera que podrán conservarse durante períodos más largos siempre que se traten exclusivamente para dichos fines.

Principios de protección de datos

Principio de integridad y seguridad: los datos personales serán tratados de manera que se garantice su adecuada seguridad, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, aplicando las medidas técnicas y de organización apropiadas.

De acuerdo a este principio, los que traten datos personales deben actuar proactivamente con el objetivo de protegerlos frente a cualquier riesgo que amenace su seguridad.

Ejemplo: Para garantizar la seguridad de los datos personales por internet, es recomendable que el envío se realice de forma cifrada.

Principios de protección de datos

Deber de confidencialidad

Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad.

Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

ROLES en la PROTECCION de DATOS en una EMPRESA

Responsable del tratamiento: determina los fines y medios del tratamiento. Es decir, es quien debe informar sobre la finalidad del tratamiento.

Encargado del tratamiento: realiza el tratamiento de datos por cuenta del responsable.

En ocasiones quien posee los datos personales (responsable) puede encargar a un tercero (encargado del tratamiento), la prestación de un servicio para el cual sea necesario utilizar los datos de los clientes, cumpliendo una serie de requisitos.

Ejemplos:

- cuando la Administración encarga a una empresa que controle el área de servicio auto-regulado de aparcamiento.
- la actividad que realizan las denominadas empresas de recobro para tratar de cobrar una deuda.

Seguridad

Cualquier responsable que recabe y trate datos de carácter personal debe adoptar una serie de medidas de seguridad, de carácter técnico y organizativo para proteger los datos.

Algunas de estas medidas son:
- evitar accesos no autorizados.
- realizar copias de seguridad.
- seudonimización y cifrado de datos.
- control del almacenamiento, de los usuarios, de los soportes y del acceso a los datos.

Asimismo, **todo aquel que intervenga en la gestión o tratamiento de datos personales** debe cumplir con el deber de secreto.

! Si se produce una quiebra de seguridad que afecte a datos personales, hay que comunicarlo a los clientes y a la AEPD.

Regla general

Prohibición de tratamiento de datos que revelen el origen étnico o racial, las opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, así como el tratamiento de datos genéticos, biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud, vida sexual u orientaciones sexuales de una persona física.

Excepciones a la regla general

→ Consentimiento del titular de los datos, excepto que por el Derecho de la Unión o Estados miembros no se pueda levantar la prohibición.
→ Tratamiento necesario para que el responsable cumpla con obligaciones de Derecho laboral, seguridad y protección social, si así lo autoriza el Derecho de la Unión o convenio colectivo.
→ Tratamiento necesario para proteger el interés vital del interesado u otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para prestar su consentimiento.
→ Tratamiento realizado por una fundación, asociación u otra entidad sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera a sus miembros (antiguos o actuales) o personas que mantegan contactos regulares, y que los datos no se cedan a terceros sin consentimiento.
→ Tratamiento referido a datos que el interesado ha hecho manifiestamente públicos.
→ Tratamiento necesario para la formulación, ejercicio o defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función.
→ Tratamiento necesario en base al interés público esencial, sobre la base del Derecho (UE o Estados miembros), debiendo ser proporcional al objetivo perseguido, respetando la protección de datos y estableciendo medidas para proteger los intereses y derechos fundamentales del interesado.
→ Tratamiento para fines de medicina (preventiva/laboral), evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación/tratamiento sanitario o social o gestión de sistemas y servicios de asistencia sanitaria.
→ Tratamiento necesario por razones de interés público en el ámbito de la salud pública o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos/productos sanitarios, sobre la base del Derecho (UE o Estados miembros), adoptando medidas adecuadas para proteger los derechos y libertades del interesado, en particular el secreto profesional.
→ Tratamiento con fines de archivo en interés público, investigación científica, histórica o estadística, respetando la protección de datos y estableciendo medidas para proteger los intereses y derechos fundamentales del interesado.

Derechos del usuario

Derecho de información.

Derecho de acceso.

Derecho de rectificación.

Derecho de oposición.

Derecho de supresión.

Derecho a no ser objeto de decisiones individualizadas.

Derecho de información (transparencia)

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

- Su ejercicio es gratuito.
- Si las solicitudes son manifiestamente infundadas o excesivas (carácter repetitivo) el responsable podrá cobrar un canon proporcional a los costes administrativos soportados.
- Deben responderse en el plazo de un mes.
- Se puede prorrogar otros dos meses más, teniendo en cuenta la complejidad y número de solicitudes.
- El responsable está obligado a informar sobre los medios para ejercitar estos derechos.

Derecho de información (transparencia)

Cuando se recaben tus datos de carácter personal el responsable del tratamiento debe facilitar al afectado determinada información:

- identidad del responsable del tratamiento.
- finalidad del tratamiento (ejemplo, si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles).
- posibilidad de ejercer los derechos establecidos.

Esta obligación de informar se debe cumplir sin necesidad de requerimiento alguno, y el responsable deberá poder acreditar con posterioridad que ha sido satisfecha

Derecho de información (transparencia)

Ejemplos:

- cuando en una página web se realiza recogida de datos personales se deberá informar de lo anteriormente descrito. En muchas ocasiones, esta información se encuentra disponible en el apartado inferior de estas páginas web bajo el título “Política de privacidad”, “Términos y Condiciones” o “Aviso legal”.

- si se usa un GPS en el coche de empresa con una finalidad de control, también se ha de informar con carácter previo a su puesta en funcionamiento.

Derecho de información (transparencia)

Cuando se navega por internet y se visitan páginas web, éstas introducen las denominadas cookies, que suponen la descarga de un archivo o dispositivo en el terminal que, en muchas ocasiones, se utilizan para realizar perfiles de navegación de los usuarios. En este sentido, también te deben informar de la instalación de determinadas cookies y de su finalidad. Esta información aparece en las páginas web bajo la denominación ‘Aviso de cookies’ o ‘Política de cookies’.

Derecho de acceso

Derecho del usuario a dirigirse al responsable del tratamiento para conocer:

- si está tratando o no sus datos de carácter personal.
- obtener copia de los datos personales que son objeto de tratamiento.
- fines del tratamiento.
- destinatarios a los que se comunicaron o serán comunicados sus datos personales.
- plazo previsto de conservación de los datos personales o, si no es posible, los criterios utilizados para determinar este plazo.
- cuando los datos personales no se hayan obtenido directamente del usuario, cualquier información disponible sobre su origen.
- existencia de decisiones automatizadas, incluida la elaboración de perfiles, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Derecho de rectificación

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

Derecho de oposición

Este derecho supone que el usuario puede oponerse a que el responsable realice un tratamiento de sus datos personales.

Derecho de supresión/cancelación

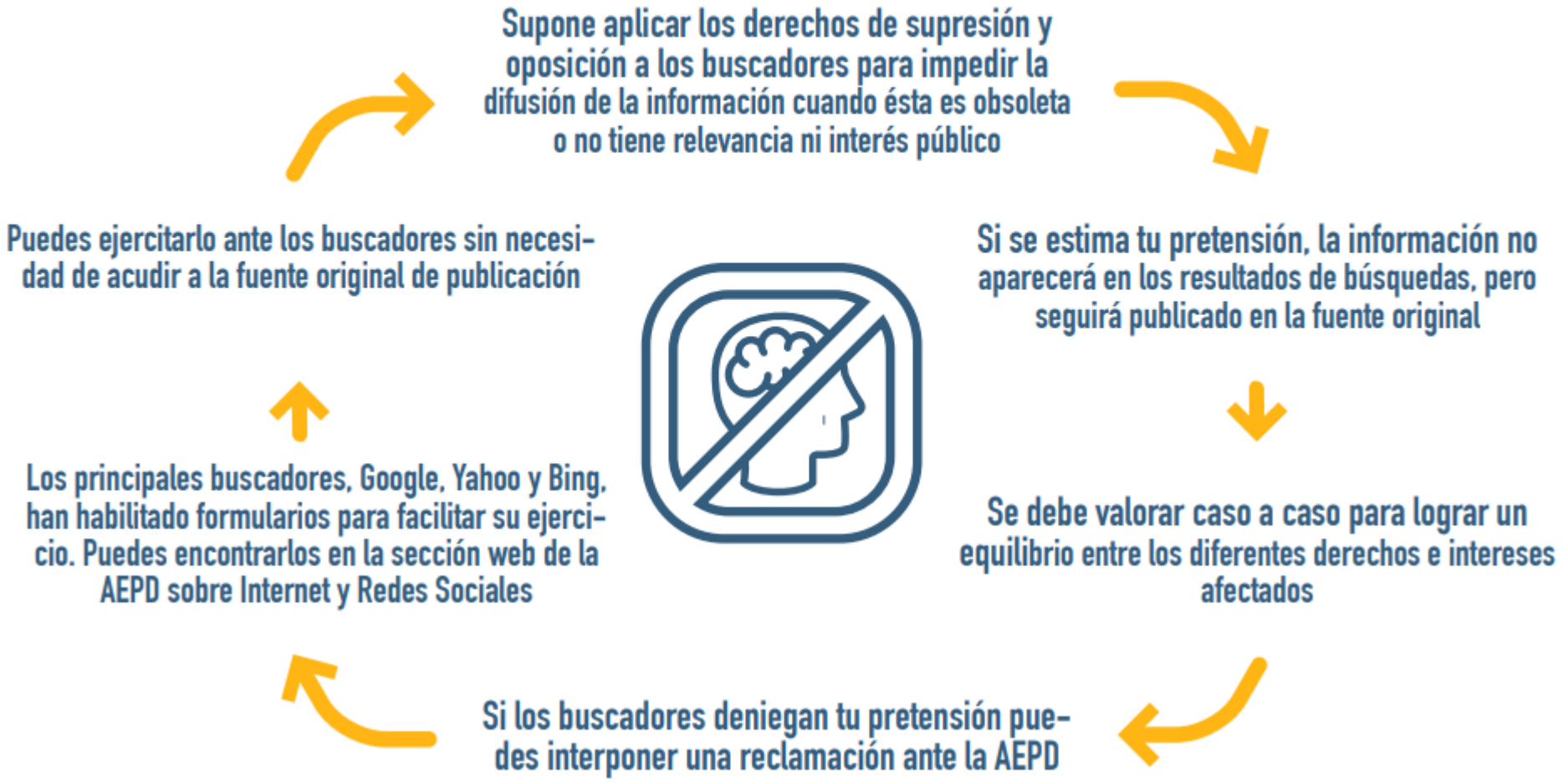
Podrá ejercitarse este derecho ante el responsable solicitando la supresión de sus datos de carácter personal, si los datos ya no son necesarios en relación con los fines para los que fueron recogidos.

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.
- cumplimiento de una obligación legal.
- razones de interés público.
- ámbito de la salud pública.
- fines de investigación científica o histórica.
- fines estadísticos

En este sentido, la AEPD fue pionera al considerar que el tratamiento de datos que realizan los motores de búsqueda de internet, como Google, Bing o Yahoo, está sometido a la normas de protección de datos de la Unión Europea, y que los ciudadanos pueden solicitar, bajo ciertas condiciones, que los enlaces a sus datos personales no aparezcan en los resultados de una búsqueda realizada por su nombre y apellidos.

Datos de buscadores



Derecho a no ser objeto de decisiones individualizadas

Este derecho pretende garantizar que no el usuario no sea objeto de una decisión basada únicamente en el tratamiento de sus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre él o le afecte significativamente.

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

No obstante, este derecho no será aplicable cuando:

- sea necesario para la celebración o ejecución de un contrato.
- el tratamiento de los datos se fundamente en consentimiento prestado previamente.

No obstante, el responsable deber garantizar el derecho a obtener la intervención humana, expresar tu punto de vista e impugnar la decisión.

¿Qué necesita hacer una empresa para cumplir con la nueva LOPD?

- Crear el registro de actividades del tratamiento (RAT).
- Establecer protocolos de ejercicios de derecho, modelos de ejercicio y modelos de respuesta.
- Establecer protocolos de declaración de brechas.
- Contratos de confidencialidad y obligaciones RGPD para trabajadores y colaboradores.
- Contratos de encargo de tratamiento con terceros.
- Cláusulas específicas de información de uso obligatorio a incluir en todos los formularios.

Ref: https://www.ciudadano2cero.com/ley-proteccion-datos-rgpd/

Crear tu registro de actividades del tratamiento (RAT)

- Aunque el término suena rimbombante, éste es **un simple documento interno** que define todos los tratamientos que realizas y las medidas de seguridad que aplicas.

- Es un documento obligatorio y puede ser requerido por la autoridad de control (la agencia de protección de datos) en cualquier momento. Deberá estar actualizado en todo momento.

Ref: https://www.ciudadano2cero.com/ley-proteccion-datos-rgpd/

Establecer protocolos de ejercicios de derecho, modelos de ejercicio y modelos de respuesta

Esto es algo básico para responder a los derechos que tienen los ciudadanos sobre su información personal, derechos a acceder, rectificar, limitar, oponerse o suprimir la información que le pertenece.

¿Podrías atender eficazmente a estos derechos si alguien te lo requiriera ahora mismo?

Es algo vital que sepas hacerlo, hay un plazo legal para dar respuesta y **la negativa a responder es una infracción grave**.

Ref: https://www.ciudadano2cero.com/ley-proteccion-datos-rgpd/

Establecer protocolos de declaración de brechas

El RGPD exige que siempre **que tengas conocimiento de una brecha de seguridad** que exponga información personal de otros tratada bajo tu responsabilidad.

Debes **poner en conocimiento** de esa brecha **a la agencia de protección de datos y a los propios afectados;** es decir, debes comunicar a esas personas que sus datos han sufrido un ataque para que tomen las medidas necesarias (cambiar contraseñas, etc).

Ref: https://www.ciudadano2cero.com/ley-proteccion-datos-rgpd/

Contratos de confidencialidad y obligaciones RGPD para trabajadores y colaboradores

Una cuestión básica es **informar a todas las personas que tienen acceso a información de terceros sobre sus obligaciones y responsabilidad** respecto al tratamiento de datos que realizan.
Se trata de crear una cultura de protección de datos en tu organización, porque de poco servirán las mejores medidas de seguridad **si tus empleados no las conocen**.

Están a la orden del día infracciones graves como utilizar datos personales de una base de datos con fines distintos a los informados u organizar una campaña de captación sin saber cuáles son requisitos legales para ello (es decir, informando y requiriendo el consentimiento previo).

Ref: https://www.ciudadano2cero.com/ley-proteccion-datos-rgpd/

Contratos de encargo de tratamiento con terceros

Otro aspecto clave en el cumplimiento es que **regules las relaciones con los encargados de tratamientos**, es decir, personas o autónomos con los que compartes información personal del que eres responsable; por ejemplo, tu gestoría, tu webmaster, la empresa de mensajería, etc.

El RGPD exige que elijas sólo a aquellos que ofrezcan las máximas garantías de tratamiento y, para ello, deben firmar un contrato que exprese los límites en el tratamiento y los deberes y obligaciones que tienen respecto a esos datos.

También tendrás que pedirles que acrediten cumplimiento; puedes mandarles un formulario para evaluarlos o pedirles pruebas específicas, como el RAT, capturas, etc.

Ref: https://www.ciudadano2cero.com/ley-proteccion-datos-rgpd/

Cláusulas específicas de información de uso obligatorio a incluir en todos los formularios

Debes incluir estas cláusulas **en los lugares de captura de datos personales**, en función de la **finalidad** de la información recogida.

Adaptar tu página web a todas las exigencias del RGPD y la nueva LOPD

Tu web debería disponer de algunos textos básicos:

- Política de privacidad.
- Aviso legal.
- Política de cookies.

Ref: https://www.ciudadano2cero.com/ley-proteccion-datos-rgpd/

Las sanciones de la Ley de Protección de datos de carácter personal

En la LOPD se hace una clasificación entre **infracciones muy graves, graves y leves**.

Las sanciones han aumentado notablemente: el importe máximo está en los **20 millones de euros o el 4% de la facturación bruta anual**, lo que sea mayor.

Además, cualquier afectado puede requerir, además de la sanción, **una indemnización** si se demuestra que sus derechos se han visto vulnerados.

Ref: https://www.ciudadano2cero.com/ley-proteccion-datos-rgpd/