LEGÁLITAS

RECOMENDACIONES PARA EL CUMPLIMIENTO EN MATERIA DE PROTECCION DE DATOS

Diferencias relevantes respecto de la normativa anterior:

LOPD 1999	RGPD	LOPDGDD
• Consentimiento entendido como "manifestación de voluntad". • Ficheros. • Documento de seguridad. • Datos especialmente protegidos. • Derechos ARCO. • Medidas de seguridad básicas, medias y altas.	• Consentimiento entendido como "declaración" o "clara acción afirmativa". • Inventario de tratamientos. • Principio de resp. proactiva y transparencia. • Categorías especiales de datos personales. • Nuevos derechos (portabilidad, limitación de tratamiento, oposición a la elaboración de perfiles, derecho al olvido). • Evacuaciones de impacto (PIA's) (tratamientos a gran escala de datos personales y/o tecnologías intrusivas para la privacidad).	• Derechos digitales: olvido y portabilidad en redes sociales, testamento digital, desconexión digital e intimidad en el ámbito laboral, acceso universal a internet, educación digital, etc.

01. OBLIGACIONES FORMALES

Todo encargado del tratamiento tendrá que cumplir con una serie de obligaciones formales, entre las que se encuentran las siguientes:

Inventario de Tratamientos

Desaparece la obligación de notificar el registro de ficheros al Registro General de la AEPD.
Aparece la obligación de elaborar un Inventario de Tratamiento de Datos Personales.

Análisis de Riesgos

Se debe realizar Análisis de Riesgos para la definición de las medidas de seguridad aplicables al tratamiento de datos personales.

Evaluación de impacto relativa a protección de datos

Se debe realizar Análisis de Riesgos para la definición de las medidas de seguridad aplicables al tratamiento de datos personales.

Delegado de Protección de Datos (DPD)

La empresa deberá nombrar un Delegado de Protección de datos en el caso en el que la compañía realice un monitoreo de datos de carácter personal sensibles o bien procese grandes cantidades de categorías especiales de datos personales.

Relaciones con Terceros. Contratos de Encargo de Tratamiento

Se deben regularizar a través de un contrato por escrito, las relaciones con terceros con acceso de datos personales, que incluya las nuevas exigencias del RGPD.
Los Encargados de Tratamiento deberán realizar Evaluaciones de Impacto, en concordancia con los Responsables del Tratamiento.

Obligada notificación de violaciones de seguridad

Las organizaciones deben notificar a la autoridad de control de protección de datos en caso de violaciones de seguridad sin demora injustificada, en el plazo máximo de 72 horas, salvo que no suponga un riesgo alto para los derechos y libertades del afectado.

Si existe un riesgo alto para los afectados, éstos también deberán ser informados.

Privacidad desde el diseño y por defecto

Las organizaciones deben considerar las necesidades de protección de datos en el diseño de productos y servicios que pretendan lanzar al mercado, y garantizar la seguridad por defecto.
En resumen, se exige a la empresa una RESPONSABILIDAD PROACTIVA y TRANSPARENCIA.

La **responsabilidad proactiva** exige una "actitud consciente, diligente y proactiva" por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

El RGPD describe este principio como 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 norma.
De acuerdo con la AEPD, 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.

Además, el RGPD adopta un enfoque proactivo, exigiendo que el responsable adopte medidas **preventivas** dirigidas a reducir los riesgos de incumplimiento y, además, que esté en condiciones de demostrar que ha implantado esas medidas y que las mismas son las adecuadas para lograr la finalidad perseguida.

Son ejemplos de este tipo de medidas: el Delegado de protección de datos, el Registro de actividades de tratamiento, las evaluaciones de impacto sobre protección de datos, etc.

Estas medidas se completan con los derechos de los afectados respecto al tratamiento de sus datos personales, la relación entre el responsable y el encargado de tratamiento, así como la legitimación para el tratamiento de los datos personales.

02. RECOGIDA DE DATOS

La recogida de datos de carácter personal deberá hacerse de acuerdo siempre a los principios básicos recogidos en la normativa sobre privacidad.

Estos principios son: la calidad de los datos, consentimiento del afectado, deber de secreto, derecho de información en la recogida de datos y seguridad de los datos.

PRINCIPIO DE CALIDAD DE LOS DATOS

Los datos solo podrán ser recogidos o tratados cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
Asimismo, los datos de carácter personal no podrán usarse para finalidades distintas de las que han sido obtenidos y siempre deberán ser exactos y puestos al día para que reflejen la situación real del afectado.

CONSENTIMIENTO DEL AFECTADO

Desaparece el consentimiento tácito. El consentimiento debe ser inequívoco y 'explícito' en el caso de categorías especiales de datos personales o de producirse una transferencia internacional de datos.

El consentimiento del afectado debe darse libremente y para finalidades específicas.
Los clientes deben estar informados sobre la opción de revocar su consentimiento.
Corresponde a aquel que recaba los datos, probar que el consentimiento se ha otorgado de forma adecuada.

Hay que tener en cuenta que el consentimiento es revocable en cualquier momento por el interesado, sin que tenga efectos retroactivos.

Es importante conocer que lo referente al consentimiento queda claramente definido en el considerando 32 del RGPD, y ha supuesto uno de los mayores cambios respecto a la legislación actual:

> *"El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento."*

SEGURIDAD DE LOS DATOS

La empresa ha de garantizar la seguridad de los datos de carácter personal, adoptando las medidas técnicas y organizativas necesarias, evitando, en todo caso su alteración, pérdida, tratamiento o acceso no autorizado.

La empresa deberá de forma proactiva, desde el diseño y por defecto, analizar los riesgos de cada tratamiento en función de la sensibilidad de los datos y del volumen de los mismos, y en consecuencia adoptar medidas minimizadoras del riesgo, tales como anonimización, pseudonimización, cifrado de comunicaciones datos sensibles y otras que resulten adecuadas para garantizar la seguridad de los datos.

DEBER DE INFORMACION

La AEPD recomienda adoptar un modelo de información por capas o niveles. Consiste en presentar una información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos y remitir a la información adicional en un segundo nivel, donde se presentarán detalladamente el resto de las informaciones, en un medio más adecuado para su presentación, comprensión y, si se desea, archivo.

El deber de información debe comprender los siguientes puntos:

- La existencia del tratamiento, su finalidad y destinatarios.
- El carácter obligatorio o no de la respuesta, así como de sus consecuencias.
- La posibilidad de ejercitar los derechos de privacidad (antiguos derechos ARCO más los nuevos de RGPD).
- La identidad y datos de contacto del responsable del tratamiento.
- Los datos de contacto del Delegado de Protección de Datos, en su caso,
- La base jurídica o legitimación para el tratamiento,
- El plazo o los criterios de conservación de la información,
- La existencia de decisiones automatizadas o elaboración de perfiles.
- La previsión de transferencias a Terceros Países.
- El derecho a presentar una reclamación ante las Autoridades de Control.

Y además, en el caso de que los datos no se obtengan del propio interesado:

- El origen de los datos.
- Las categorías de los datos.

La información se debe poner a disposición de los interesados **en el momento en que se soliciten los datos**, previamente a la **recogida o registro**, si es que los datos se obtienen directamente del interesado.

En el caso de que los datos no se obtengan del propio interesado, por proceder de alguna cesión legítima, o de fuentes de acceso público, el Responsable informará a las personas interesadas **dentro de un plazo razonable**, pero en cualquier caso antes de un mes desde que se obtuvieron los datos personales, o bien antes o en la primera comunicación con el interesado, antes de que los datos, en su caso, se hayan comunicado a otros destinatarios.

Únicamente no será necesario informar **cuando el interesado ya disponga de la información**, ni tampoco, en el caso de que los datos no procedan del interesado en casos tasados como cuando la comunicación resulte imposible o suponga un esfuerzo desproporcionado.

La AEPD facilita el siguiente modelo de información por capas:

Epígrafe	Información Básica (1ª capa, resumida)	Información Adicional (2º capa, detallada)
"Responsable" (del tratamiento)	• Identidad del responsable de tratamiento.	• Datos de contacto del responsable. Identidad y datos del representante. • Datos de contacto del Delegado de Protección de Datos.
"Finalidad" (del tratamiento)	• Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles.	• Descripción ampliada de los fines del tratamiento Plazos o criterios de conservación de los datos. • Desiciones automatizadas, perfiles y lógica aplicada.
"Legitimación" (del tratamiento)	• Base jurídica del tratamiento.	• Detalle de la base jurídica del tratamiento, en los casos de oblicación legal, interés público o interés legítimo.
"Destinatarios" (de cesiones o transferencias)	• Previsión o no de Cesiones • Previsión de transferencias, o no, a terceros países.	• Destinatarios o categorías de destinatarios. • Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables.
"Derechos" (de las personas interesadas)	• Referencia al ejercicio de derechos.	• Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento. • Derechos a retirar el consentimiento prestado. • Derecho a reclamar ante la Autoridad de Control.
"Procedencia" (de los datos)	• Fuente de los datos (cuando no proceden del interesado).	• Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público. Categorías de datos que se traten.

DEBER DE SECRETO

El personal de la empresa y, en general, cualquiera que tenga acceso a los datos personales está obligado a guardar secreto profesional con respecto a los mismos.

CATEGORÍAS ESPECIALES DE DATOS

La LOPD incluía unas categorías de datos a los que llamaba "datos especialmente protegidos", que básicamente son los mismos que ahora el RGPD denomina "categorías especiales de datos".

Se trata, según define el considerando 51 de *"los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, merecen especial protección ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales".*

La regla general es la **prohibición** de tratar ese tipo de datos, si bien se establecen excepciones a esta prohibición, tales como que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física, y el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento o cuando se refiera a datos personales que el interesado ha hecho manifiestamente públicos.

Otro de los supuestos en los que se **excepciona esta prohibición** es que el interesado consienta de manera explícita (salvo que otra norma de la UE o de algún estado miembro indique que no es suficiente el consentimiento en ese caso). Eso ocurre por ejemplo en España ya que la vigente Ley Orgánica de Protección de Datos Personales y Gestión de Derechos Digitales indica que *"el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico"*, siendo por tanto necesario que se de alguno de los restantes supuestos contemplados como excepción en el RGPD para poder realizar el tratamiento de esos datos.

Entran en esta categoría los 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**.

El RGPD incluye dos categorías de datos dentro de estos datos que requieren una especial protección respecto de los existentes en la LOPD anterior.

- Los **datos genéticos**, provenientes del análisis de una muestra biológica en particular a través de un análisis del ADN o del ARN o equivalente.
- Los **datos biométricos** que son los que se obtienen a partir de un tratamiento técnico específico que permitan una identificación única de la persona, como la huella dactilar. En este sentido, es importante llamar la atención a las empresas que tenían entre sus procesos de acceso la identificación mediante un lector de huellas, para que analicen si ese tratamiento, que ahora afecta a un dato calificado como de categoría especial, se realiza conforme a la normativa actual.

Por otra parte, aunque los datos relativos a la vida sexual ya venían contemplados en la LOPD como datos especialmente protegidos, ahora se han hecho extensivos también a "la orientación sexual", por lo que se incluyen a partir del RGPD en esa categoría todos aquellos datos que pudiera revelar la orientación sexual de la persona.

TRANSFERENCIAS INTERNACIONALES

Las transferencias internacionales de datos suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo, formado por los países de la Unión Europea más Liechtenstein, Islandia y Noruega.

Los responsables y encargados del tratamiento podrán realizar transferencias internacionales de datos sin necesidad de una autorización de la Agencia Española de Protección de Datos siempre que el tratamiento de datos observe lo dispuesto en el RGPD y se den los siguientes supuestos.

1. Que el destinatario haya sido declarado de nivel adecuado por la Comisión Europea.
2. A falta de decisión de adecuación, que se den una serie de garantías como que haya normas corporativas vinculantes o se utilicen cláusulas tipo de protección de datos adoptadas por la Comisión, que siguen siendo válidas.
   Se necesitará autorización expresa de la AEPD cuando las garantías sean las siguientes:
   a) cláusulas contractuales entre el responsable o el encargado y el responsable, y el encargado y subencargado, que no hayan sido adoptadas por la Comisión Europea o
   b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

Las autorizaciones otorgadas por la Agencia Española de Protección de Datos previamente a la aplicación del RGPD seguirán siendo válidas.

3. A falta de decisión de adecuación y de garantías solo se podrá dar si se cumple alguna de una lista cerrada de condiciones, como por ejemplo que el interesado haya dado explícitamente su consentimiento o que la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones.

Cuando tampoco sea aplicable ninguna de estas excepciones, solo se podrá llevar a cabo una transferencia si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evalué todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofrezca garantías apropiadas con respecto a la protección de datos personales.

En este supuesto el responsable del tratamiento **informará a la autoridad de control** (en España la Agencia Española de Protección de Datos con carácter general o las autonómicas en caso de que las haya) de la transferencia. Además el **interesado deberá ser informado** de este hecho y de los intereses legítimos imperiosos perseguidos con la transferencia.

Normas corporativas vinculantes (BCR)

En los casos de grupos empresariales o unión de empresas dedicadas a una actividad económica conjunta se ha previsto la posibilidad de solicitar a la Agencia la aprobación de Normas Corporativas Vinculantes (o BCR por sus siglas en inglés) para realizar este tipo de transferencias entre sus componentes.

COMUNICACIONES COMERCIALES

la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico prohíbe el envío de comunicaciones publicitarias o promocionales por medios electrónicos que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. Esto es aplicable también a otros canales de comunicación, y no solo los electrónicos.

Existe una excepción a esta prohibición: *cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.*

Es importante tener en cuenta que SIEMPRE deberá ofrecerse al destinatario la posibilidad de **oponerse** al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Además, cuando las comunicaciones comerciales se realicen por vía electrónica, ya sea dirigido a personas físicas o jurídicas, será necesario:

- Identificar claramente que se trata de una comunicación de carácter comercial, así como la identidad de la persona que la realiza.
- Informar al destinatario de la comunicación del origen de sus datos

EJERCICIO DE DERECHOS

El responsable del tratamiento facilitará a los interesados el ejercicio de sus derechos, así como procedimientos para ello visibles, accesibles, sencillos y gratuitos (salvo excepciones para determinados supuestos). Deberá informar al interesado sobre las actuaciones derivadas de su petición en el plazo de un mes, que se podrá extender dos meses en algunos casos, como cuando se trate de solicitudes especialmente complejas, notificando esa ampliación dentro del primer mes.

Derecho de Acceso

Es el derecho del interesado a obtener del responsable del tratamiento, confirmación de si se están tratando o no datos personales que le conciernen, y en caso de que sea así, acceder a información como la finalidad del tratamiento, categoría de los datos personales que se tratan, destinatarios o categorías de destinatarios a los que se les comunicarán estos datos, etc.

Derecho de Rectificación

Es el derecho que tiene el interesado a solicitar del responsable del tratamiento la rectificación de sus datos cuando sean inexactos. Ante esta solicitud el responsable deberá satisfacer este derecho sin dilación indebida. Teniendo en cuenta los fines para los cuales hayan sido tratados los datos, el interesado tendrá derecho a que se completen cuando éstos resulten incompletos.

Derecho de Supresión

El derecho a la supresión (también contemplado como derecho al olvido), es la denominación que da el RGPD al tradicional derecho de cancelación. En base al mismo, el interesado tendrá derecho a obtener, sin dilación indebida del responsable del tratamiento, la supresión de los datos personales que le conciernan, cuando concurra alguna de las circunstancias siguientes:

- Cuando los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.
- Cuando el interesado retire el consentimiento en que se basa el tratamiento y este no se base en otro fundamento jurídico.
- Cuando el interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento.
- Cuando los datos personales hayan sido tratados ilícitamente.
- Cuando los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.
- Cuando los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información dirigidos a menores.

Derecho de oposición

Es el derecho del interesado a oponerse, en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento.

Ante el ejercicio del derecho de oposición el responsable del tratamiento dejará de tratar los datos personales. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines. Sin embargo, el derecho de oposición no es un derecho absoluto del interesado, por lo que procederá, en supuestos distintos de la mercadotecnia directa, realizar una ponderación con el fin de considerar si prevalece o no el derecho del interesado.

Derecho a la Portabilidad

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.

Derecho a la Limitación

El derecho a la limitación del tratamiento de los datos personales es otro de los nuevos derechos que recoge el RGPD, como "el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro". Se trata de una medida cautelar que reduce el tratamiento de los datos personales a la conservación. Los supuestos en los que el interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos, están tasados por la norma, y son, a modo de ejemplo, cuando el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos o cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

Derecho a no ser objeto de decisiones individualizadas

Es el derecho de todo interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Sin embargo, el RGPD recoge unos supuestos en los que es lícito efectuar el tratamiento y tomar una decisión automatizada:

- Cuando está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.
- Cuando sea necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento.
- Cuando se basa en el consentimiento explícito del interesado.

INFRACCIONES Y SANCIONES

Con la aprobación de la LOPDGDD se establece un régimen sancionador sujeto al establecido por el RGPD, que aplica a los siguientes sujetos:

- Responsable de tratamiento
- Encargados de tratamiento
- Representantes de responsable o encargado de tratamiento no establecidos en UE.
- Entidades de certificación
- Entidades supervisión de códigos de conducta

No aplicará al Delegado de Protección de datos.

Criterios de imposición de las multas administrativas

El RGPD establece que las sanciones se impondrán de acuerdo a las circunstancias de cada caso, y la decisión y cuantía variarán dependiendo de criterios tales como la naturaleza, gravedad y duración de la infracción o las medidas tomadas por el responsable o encargado del tratamiento para paliar los daños y perjuicios o bien otros factores atenuantes o agravantes.

Además, la LOPDGDD añade a este listado otros aspectos a tener en cuenta a la hora de la decisión y cuantía a imponer, como la reincidencia o los beneficios obtenidos como consecuencia de la comisión de la infracción, la afectación a los derechos de los menores o el sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

Tipificación de las infracciones

El RGPD recoge que las infracciones podrán ser graves o muy graves y serán sancionadas con una multa administrativa que podrá alcanzar en el primer caso la cuantía 20.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la

de mayor cuantía y en el caso de las muy graves multa administrativa que alcance una cuantía de 20.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. La LOPDGDD establece la posibilidad, además, de sanciones leves.

MUY GRAVES

El Articulo 72 LOPDGDD tipifica como infracciones muy graves, que prescribirán a los 3 años, tomando como referencia el artículo 83.5 del RGPD, entre otros:

- El tratamiento de datos personales de forma ilícita.
- El incumplimiento de los requisitos para la validez del consentimiento.
- La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos.
- El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos de los afectados.

GRAVES

El Articulo 73 LOPDGDD tipifica como infracciones graves, que prescribirán a los 2 años, tomando como referencia el artículo 83.4 del RGPD, entre otros:

- El tratamiento de datos personales de un menor de edad sin recabar el consentimiento adecuado.
- La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento.
- La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas.
- El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

LEVES

El Articulo 74 LOPDGDD tipifica como infracciones leves, que prescribirán al año, las restantes infracciones de carácter meramente formal. Entre otras, son:

- El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida en la normativa.
- No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible.
- Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el RGPD.