Proyecto de Ley Orgánica de Protección de Datos de carácter personal (PLOPD)

Gobierno de España

Índice

Introducción

En noviembre de 2017, el Gobierno publicó el Proyecto de Ley Orgánica de Protección de Datos de carácter personal, que derogará la actual LOPD con el objetivo de adaptar la legislación española al Reglamento General de Protección de Datos (GDPR)

Introducción

- La protección de las personas físicas en relación con el **tratamiento de datos personales** es un derecho fundamental que garantiza a las personas el control sobre sus datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados. De esta forma, este derecho se configura como una facultad para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención.
- Con el objetivo de impulsar una regulación más uniforme de este derecho fundamental, el Parlamento Europeo y el Consejo aprobaron en abril de 2016 el Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos (**GDPR**), que será aplicable a partir del **25 de mayo de 2018**.

- En este contexto, tras la publicación del Anteproyecto de Ley (APLOPD) en junio de 2017, el Gobierno publicó en noviembre de 2017 el **Proyecto de Ley Orgánica de Protección de Datos (PLOPD)**, que derogará la actual LOPD, y que adaptará la legislación española a las disposiciones del GDPR, introduciendo novedades y mejoras en la regulación de este derecho fundamental.
- Los aspectos más relevantes que recoge el PLOPD son los siguientes:
  - Disposiciones generales
  - Principios de protección de datos
  - Derechos de las personas
  - Disposiciones aplicables a tratamientos concretos
  - Responsable y encargado del tratamiento
  - Transferencias internacionales de datos
  - Autoridades de protección de datos, como la Agencia Española de Protección de Datos (AEPD)
  - Procedimientos en caso de posible vulneración de la normativa de protección de datos
  - Régimen sancionador

En esta Nota Técnica se resume el contenido de este Proyecto de Ley Orgánica.

Índice

Resumen ejecutivo

Contenido de la norma

Los aspectos más relevantes del GDPR que aborda este Proyecto de Ley son: principios, derechos, tratamientos, responsable y encargado del tratamiento, transferencia internacional de datos, autoridades, procedimientos en caso de vulneración y régimen sancionador

Contenido de la norma

Ámbito de aplicación

- El PLOPD se aplica a cualquier **tratamiento total o parcialmente automatizado** de datos personales, así como al **tratamiento no automatizado de datos personales** contenidos o destinados a ser incluidos en un fichero.

Contexto normativo

- **Reglamento (UE) 2016/679 (GDPR)**, del Parlamento Europeo y del Consejo (abril, 2016).
- **Ley Orgánica 15/1999**, **de Protección de Datos de carácter personal (LOPD)** de las Cortes Generales (Diciembre, 1999).

Próximos pasos

- Una vez aprobada la nueva Ley Orgánica, ésta entrará en vigor el **25 de mayo de 2018**, derogando la actual LOPD a partir de esa fecha.

Contenido de la norma

1. **Disposiciones generales**: ámbito de aplicación, excepciones y datos de personas fallecidas.
2. **Principios de protección de datos**: principios generales (ej. inexactitud, confidencialidad, consentimiento).
3. **Derechos de las personas**: transparencia e información al afectado, ejercicio de derechos (ej. acceso, supresión).
4. **Disposiciones aplicables a tratamientos concretos**: información crediticia, videovigilancia, exclusión publicitaria, etc.
5. **Responsable y encargado del tratamiento**: obligaciones, registro de actividades, delegado de protección de datos, etc.
6. **Transferencias internacionales de datos**: régimen de transparencia y determinados supuestos (ej. adopción por AEPD).
7. **Autoridades de protección de datos**: AEPD (i.e. facultades y potestades) y autoridades autonómicas.
8. **Procedimientos en caso de posible vulneración de la normativa de protección de datos**: régimen, procedimiento y plazo.
9. **Régimen sancionador**: sujetos responsables, infracciones (muy graves, graves, leves) y sanciones.

Índice

Detalle

Disposiciones generales

La futura ley se aplicará a cualquier tratamiento total o parcialmente automatizado de datos personales y al tratamiento no automatizado de datos personales incluidos en un fichero. Además, se incluye como novedad la regulación del uso de datos de personas fallecidas

Disposiciones generales

Ámbito de aplicación[1]

- Cualquier **tratamiento total o parcialmente automatizado de datos personales**.
- El **tratamiento no automatizado** de datos personales contenidos o destinados a ser incluidos en un **fichero**.

Excepciones

- Los tratamientos efectuados por una persona física en el ejercicio de **actividades exclusivamente personales o domésticas**.
- Los tratamientos llevados a cabo por los órganos de la **Administración General del Estado** en el marco de ciertas actividades sobre **política exterior** y **seguridad común**.
- Los tratamientos por parte de las autoridades competentes y sus agentes con fines de **prevención**, **investigación**, **detección o enjuiciamiento de infracciones penales**, o **ejecución de sanciones penales**, incluida la protección frente a amenazas a la seguridad pública y su prevención.
- Los tratamientos de **datos de personas fallecidas**, sin perjuicio de lo previsto a continuación.
- Los tratamientos sometidos a la normativa sobre protección de materias clasificadas (ej. secretos oficiales).

Datos de personas fallecidas

- Los **herederos de una persona fallecida** que acrediten dicha condición podrán dirigirse al responsable o encargado del tratamiento para solicitar el acceso, rectificación o supresión de los datos personales de aquella, salvo si la persona fallecida lo hubiese prohibido expresamente o si así lo establece una ley.
- Estos derechos también podrán ser ejercidos por el **albacea testamentario** o por aquella persona o institución a la que el fallecido hubiese conferido un mandato expreso.
- El **Ministerio Fiscal** ejercerá estas facultades en caso de fallecimiento de menores o personas con discapacidad.

(1) Los tratamientos en los que no sea directamente aplicable el GDPR, se regirán por la legislación específica que hubiese y supletoriamente por el GDPR y este PLOPD.

Detalle

Principios de protección de datos

Se establece la no imputación de la inexactitud de los datos personales al responsable del tratamiento y se exige un consentimiento expreso, así como un deber de confidencialidad. Además se reduce de 14 a 13 años la edad a partir de la cual se puede prestar consentimiento

Principios generales de protección de datos

Inexactitud

- No serán imputables al responsable del tratamiento los **datos personales inexactos**, con respecto a los fines para los que se tratan[1], siempre que éste haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación.

Confidencialidad

- Los **responsables y encargados del tratamiento de datos** así como todas las personas que intervengan en cualquier fase del mismo, estarán sujetas al deber de confidencialidad previsto en el GDPR, que será complementario a los **deberes de secreto profesional**.
- Estas obligaciones se mantendrán, aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Tratamiento basado en el consentimiento

- El consentimiento del afectado es toda **manifestación de voluntad libre**, **específica**, **informada e inequívoca** por la que éste acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Consentimiento de menores de edad

- El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea **mayor de 13 años**, salvo que la ley exija la asistencia de los titulares de la patria potestad o tutela.
- El tratamiento de los datos de los **menores de 13 años** sólo será lícito si consta el consentimiento del titular de la patria potestad o tutela, con el alcance que ellos mismos determinen.

Categorías especiales de datos

- De conformidad con el GDPR, el mero 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**.
- Por otro lado, el tratamiento de ciertos datos (ej. por razones de interés público esencial o para fines de medicina preventiva o laboral) deberán estar **amparados en una ley**.

(1) i.e. la inexactitud de los datos obtenidos directamente del afectado; la inexactitud de los datos que el responsable obtiene del mediador o intermediario; y la inexactitud de los datos procedentes del ejercicio del derecho a la portabilidad.

Detalle

Derechos de las personas

Se adopta el principio de transparencia conforme al GDPR que regula el derecho de los afectados a ser informados acerca del tratamiento de sus datos personales y se recogen, entre otros, los derechos de acceso…

Derechos de las personas (1/2)

Transparencia e información al afectado

- En los datos de carácter personal obtenidos del afectado a través de **redes de comunicaciones electrónicas** o en el marco de la prestación de un servicio de la sociedad de la información[1], el responsable del tratamiento deberá facilitar la siguiente información básica:
  - La **identidad del responsable del tratamiento** o de su representante, en su caso.
  - La **finalidad del tratamiento**.
  - El modo en que el afectado podrá **ejercitar los derechos** establecidos en el GDPR.
- Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica incluirá esta circunstancia, en cuyo caso deberá ser informado de su derecho a oponerse a la adopción de **decisiones individuales automatizadas** que pudieran afectarle significativamente.
- Adicionalmente, si los datos no hubiesen sido obtenidos del afectado la información básica incluirá también las categorías de datos objeto de tratamiento y las fuentes de la que procedieran los datos.

Ejercicio de derechos

- El responsable del tratamiento estará obligado a informar al afectado sobre los **medios para el ejercicio de sus derechos**, que no podrán ser denegados por el solo motivo de optar el afectado por otro medio.

Derecho de acceso

- Cuando el responsable trate una **gran cantidad de información** relativa al afectado y el derecho de acceso se ejercita sin especificar si se refiere a **todos o a una parte de los datos**, el responsable podrá solicitar al interesado que especifique su solicitud.
- El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un **sistema de acceso remoto**, **directo y seguro** a los datos personales.
- Se podrá considerar **repetitivo** el ejercicio de este derecho en más de una ocasión durante el plazo de 6 meses, en cuyo caso y según el GDPR se podrá: i) cobrar un canon razonable en función de los costes administrativos, y ii) negarse a actuar respecto a la solicitud.

(1) Así como en aquellos otros supuestos expresamente establecidos por la ley o cuando así lo autorice la AEPD.

Detalle
Derechos de las personas

…rectificación, supresión (‘olvido’), limitación del tratamiento, portabilidad y oposición

Derechos de las personas (2/2)

Derecho de rectificación

- Al ejercer el derecho de rectificación reconocido en el GDPR[1], el afectado deberá indicar en su solicitud a qué **datos se refiere** y la corrección que haya de realizarse, acompañándose si es preciso de la documentación justificativa de la inexactitud o carácter incompleto de los datos tratados.

Derecho de supresión

- Este derecho se ejercerá de acuerdo con el GDPR[2]. No obstante, cuando la supresión derive del ejercicio del derecho de oposición, el responsable podrá **conservar los datos identificativos** del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Derecho a la limitación del tratamiento

- Este derecho se ejercerá de acuerdo con lo establecido en el GDPR[3].
- La **limitación en el tratamiento de los datos personales** debe constar claramente en el sistema.

Derecho a la portabilidad

- Este derecho se ejercerá de acuerdo a lo establecido en el GDPR[4], en este sentido el interesado tendrá derecho a **recibir datos personales que le incumban**, facilitados a un responsable del tratamiento y a transmitirlos a otros sin que el primero lo impida, cuando el tratamiento esté basado en el consentimiento o en un contrato que se efectúe por medios automáticos.
- Este derecho no se aplicará al tratamiento realizado en **interés público**.

Derecho de oposición

- Este derecho, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerá de acuerdo con lo establecido en el GDPR[5].
- 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 basado en el cumplimiento de una misión realizada en interés público o para la satisfacción de intereses legítimos (salvo que el responsable del tratamiento acredite motivos que prevalezcan).
- En relación con las **decisiones individuales automatizadas**, el interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado.

(1) Artículo 16 GDPR. (2) Artículo 17 GDPR. (3) Artículo 18 GDPR.
(4) Artículo 20 GDPR. (5) Artículo 21 y 22 GDPR

Detalle

Disposiciones aplicables a tratamientos concretos

El PLOPD contiene disposiciones sobre tratamientos de datos concretos. En particular sobre datos de contacto y de empresarios individuales, datos relacionados con operaciones mercantiles y el tratamiento de imágenes con fines de videovigilancia

Tratamientos concretos (1/3)

Tratamiento de datos de contacto y empresarios

- El tratamiento de los **datos de contacto de las personas físicas que presten servicios en un persona jurídica** estarán amparados por el GDPR, siempre que se cumplan los siguientes requisitos:
  - Que el tratamiento se refiera únicamente a los **datos necesarios** para su localización profesional.
  - Que la finalidad del tratamiento sea **únicamente mantener relaciones** de cualquier índole con la **persona jurídica** en la que el afectado preste sus servicios.
- Este mismo tratamiento se aplicará a los **datos relativos a los empresarios individuales** cuando se refieran a ellos en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.

Tratamiento de datos de oper. mercantiles

- Salvo prueba en contrario, el tratamiento de datos que pudieran derivarse del desarrollo de cualquier **operación de modificación estructural de sociedades** o la **aportación o transmisión de negocio** o rama de actividad empresarial será lícito (incluida su comunicación previa), siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen la continuidad en la prestación de los servicios.
- Si la operación no llegara a concluirse, la entidad cesionaria deberá proceder con carácter inmediato a la **supresión de los datos**, sin que sea de aplicación la obligación de bloqueo.

Tratamientos con fines de videovigilancia

- Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el **tratamiento de imágenes** a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones. No obstante se excluye el tratamiento de imágenes llevado a cabo por una **persona física en su propio domicilio**.
- Los datos serán suprimidos en el plazo máximo de **un mes desde su captación**, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.
- El **deber de información** previsto en el GDPR se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos.

Detalle
Disposiciones aplicables a tratamientos concretos

Asimismo, se recoge el tratamiento de datos personales relativos a sistemas de información crediticia, para el cual se deberán cumplir una serie de condiciones específicas…

Tratamientos concretos (2/3)

Sistemas de información crediticia

- El tratamiento de datos personales relativos al **incumplimiento de obligaciones dinerarias**, **financieras** o de **crédito** por sistemas comunes de información crediticia será lícito cuando se cumplan los siguientes requisitos[1]:
  - Que los datos hayan sido facilitados por el **acreedor** o por quien actúe por su cuenta o interés.
  - Que los datos se refieran a **deudas ciertas**, **vencidas y exigibles**, cuya existencia o cuantía no hubiesen sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas.
  - Que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago sobre la **posibilidad de inclusión** en dichos sistemas, con indicación de aquéllos en los que participe.
  - Que los datos se mantengan en el sistema durante un **5 años desde la fecha de vencimiento** de la obligación dineraria, financiera o de crédito y sólo en tanto persista el incumplimiento.
  - Que los datos referidos a un deudor determinado solamente puedan ser consultados en los supuestos de **contratos de crédito al consumo**, así como cuando quien consulte el sistema mantuviese una **relación contractual** con el afectado que implique el abono de una cuantía pecuniaria o éste le hubiera solicitado la **celebración de un contrato** que suponga financiación, pago aplazado o facturación periódica.
  - Que, en el caso de que se **denegase la solicitud** de celebración del contrato, o éste no llegara a celebrarse como consecuencia de la consulta efectuada, quien haya consultado el sistema informe al afectado del resultado de dicha consulta.
- Las entidades que mantengan el sistema y las acreedoras, respecto del tratamiento de los datos referidos a sus deudores, tendrán la condición de **corresponsables del tratamiento de los datos**. Le corresponde al acreedor garantizar que concurren los requisitos exigidos para la inclusión en el sistema de deuda, respondiendo de su inexistencia o inexactitud.

(1) No obstante, este tratamiento no ampara los supuestos en que la información crediticia fuese asociada por la entidad que mantuviera el sistema a informaciones adicionales relacionadas con el deudor y obtenidas de otras fuentes, a fin de llevar a cabo un perfilado del mismo mediante la aplicación de técnicas de calificación crediticia.

Detalle

Disposiciones aplicables a tratamientos concretos

…los sistemas de exclusión publicitaria y los sistemas de información de denuncias en el sector privado

Tratamientos concretos (3/3)

Sistema de exclusión publicitaria

- El tratamiento de datos de carácter personal que tengan por objeto **evitar el envío de comunicaciones comerciales** a quienes hubiesen manifestado su negativa u oposición a recibirlas será lícito. A tal efecto, podrán crearse sistemas de información, generales o sectoriales, en los que sólo se incluirán los datos imprescindibles para identificar a los afectados.
- Cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados para la remisión de comunicaciones comerciales, éste deberá informarle de los **sistemas de exclusión publicitaria existentes**, pudiendo remitirse a la información publicada por la AEPD.
- En la realización de **comunicaciones comerciales** se deberá consultar previamente los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo.

Sistemas sobre denuncia interna en sector privado

- La creación y mantenimiento de **sistemas de información** a través de los cuales se pueda informar a una entidad privada, incluso anónimamente, de la **comisión de actos o conductas contrarios** a la normativa general aplicable, será lícita.
- El acceso a dichos datos quedará limitado exclusivamente al **personal que lleve funciones de control interno**.

Detalle

Responsable y encargado del tratamiento

Por otro lado, el PLOPD incluye disposiciones relativas a la determinación de medidas técnicas y organizativas aplicables ante posibles riesgos por parte del responsable y encargado del tratamiento, a la responsabilidad en supuestos de corresponsalía bancaria y el registro

Responsable y encargado del tratamiento (1/3)

Obligaciones del responsable y del encargado

- Los responsables y encargados determinarán las **medidas técnicas y organizativas apropiadas** que deben aplicar a fin de garantizar que el tratamiento es conforme con el GDPR.
- En este sentido, éstos considerarán los **mayores riesgos** que podrían producirse en los siguientes supuestos:
  - Cuando se produce cualquier **perjuicio económico**, **moral o social significativo** para los afectados.
  - Cuando el tratamiento pudiese privar a los afectados de sus **derechos y libertades** o pudiera impedirles el ejercicio del control sobre sus datos personales.
  - Cuando el **tratamiento no es meramente incidental o accesorio** de las categorías especiales de datos o de los datos relacionados con la comisión de infracciones administrativas.
  - Cuando se evalúen los aspectos personales de los afectados con el fin de crear **perfiles personales**, mediante el análisis de su rendimiento en el trabajo, situación económica, salud, etc.
  - Cuando se lleva a cabo el tratamiento de datos de grupos de afectados en situación de **especial vulnerabilidad** (i.e. menores de edad y personas con discapacidad con medidas de apoyo).
  - Cuando se produce un **tratamiento masivo** (i.e. gran número de afectados o de cantidad de datos).
  - Cuando los datos fuesen a ser **objeto de transferencia**, con carácter habitual respecto a terceros estados u organizaciones respecto de los que no se hubiese declarado un nivel adecuado de protección.

Supuesto de corresponsalía en el tratamiento

- La determinación de la responsabilidad se realizará atendiendo a las **actividades** que efectivamente desarrolle cada uno de los **corresponsables del tratamiento**.

Registro de las actividades de tratamiento

- Los responsables y encargados del tratamiento (o en su caso sus representantes) deberán mantener el **registro de actividades de tratamiento**, salvo que se trate de empresas u organizaciones que empleen a menos de 250 personas, en cuyo caso el tratamiento no debe entrañar ningún riesgo para los derechos y libertades de los interesados, debe ser ocasional, y no debe incluir categorías especiales de datos personales.
- El registro deberá especificar, según sus finalidades, las **actividades de tratamiento** llevadas a cabo y las demás circunstancias previstas en el GDPR (ej. fines del tratamiento, descripción de interesados).
- Cuando el responsable o el encargado del tratamiento hubieran designado un **delegado de protección de datos**, deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

Detalle

Responsable y encargado del tratamiento

Además, se introduce la obligación de bloqueo que garantiza que los datos quedan a disposición de ciertas autoridades, como por ejemplo los tribunales, el Ministerio Fiscal, etc., y se especifican ciertas particularidades del encargado del tratamiento

Responsable y encargado del tratamiento (2/3)

Bloqueo de los datos

- El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su **rectificación o supresión**.
- Los datos bloqueados quedarán a disposición exclusiva del tribunal, Ministerio Fiscal u otras Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y por el plazo de prescripción de las mismas.
- Los datos bloqueados **no podrán ser tratados para ninguna finalidad distinta** de las mencionadas anteriormente.
- La AEPD y las autoridades autonómicas de protección de datos, dentro del ámbito de sus competencias, podrán fijar **excepciones a la obligación de bloqueo** en los supuestos en que la mera conservación de los datos, incluso bloqueados, pudiera generar un **riesgo elevado para los derechos de los afectados** y en los que la conservación de los datos bloqueados pudiera implicar un **coste desproporcionado** para el responsable del tratamiento.

Encargado del tratamiento

- El acceso por parte de un encargado del tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable **no se considerará comunicación de datos** siempre que se cumpla lo establecido en el GDPR.
- Tendrá la consideración de responsable y no la de encargado quien en su propio nombre establezca **relaciones con los afectados**, aun cuando exista un contrato o acto jurídico con el contenido fijado en el GDPR (ej. que garantice la confidencialidad de los datos)[1]. Se considerará como responsable a quien figurando como encargado utilizase los datos para sus propias finalidades.
- El responsable del tratamiento determinará si, cuando finalice la prestación de servicios del encargado, los datos de carácter personal deben ser **destruidos**, **devueltos al responsable** o **entregados a un nuevo encargado**. No procederá su destrucción cuando exista una previsión legal que obligue a su conservación de modo que deberán ser devueltos al responsable. Por su parte, el encargado podrá conservarlos, debidamente bloqueados, si de dichos datos pudieran derivarse responsabilidades de su relación con el responsable.

(1) Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.

Detalle

Responsable y encargado del tratamiento

Adicionalmente, el PLOPD recoge la designación de un delegado de protección de datos en determinados supuestos, quién deberá contar con una cualificación y con una posición adecuadas

Responsable y encargado del tratamiento (3/3)

Delegado de protección de datos

- Los responsables y encargados del tratamiento deberán **designar un delegado de protección de datos** si: i) el tratamiento lo lleva a cabo una autoridad u organismo público; ii) las actividades del responsable o encargado requieren una observación habitual y sistemática de los interesados a gran escala; o iii) las actividades antes mencionadas se refieren a datos personales especiales y datos relativos a condenas e infracciones penales[1].
- Se considerarán incluidas en estos supuestos ciertas **entidades** (ej. los establecimientos financieros de crédito de fomento de la financiación empresarial, las entidades aseguradoras y reaseguradoras).

Cualificación del delegado

- El delegado, sea persona física o jurídica, deberá tener **conocimientos** especializados **en Derecho** y en la **práctica de protección de datos**, y deberá cumplir con las **funciones previstas en el GDPR** (ej. asesorar sobre la evaluación del impacto relativa a la protección de datos, supervisar su aplicación).
- El cumplimiento de esto requisitos podrá demostrarse entre otros medios a través de **mecanismos voluntarios de certificación**.

Posición del delegado

- El delegado actuará como **interlocutor** ante la AEPD y autoridades autonómicas de protección de datos.
- En el ejercicio de sus funciones tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer ningún deber de confidencialidad o secreto, y **comunicará cualquier vulneración** relevante a los órganos de administración y dirección del responsable o el encargado del tratamiento.
- Cuando el delegado de protección de datos aprecie la existencia de una **vulneración relevante** en materia de protección de datos lo comunicará inmediatamente a los órganos de administración y dirección del responsable o al encargado del tratamiento.

(1) En cualquier caso se podrá designar un delegado de protección de datos voluntario.

Detalle

Transferencias internacionales de datos

En relación con las transferencias internacionales de datos, se distingue entre los supuestos de adopción por la AEPD, los sometidos a autorización previa de la AEPD y los sometidos a información previa a la autoridad competente

Transferencias internacionales de datos

Régimen de las transferencias

- Las transferencias internacionales de datos se rigen por lo dispuesto en el GDPR así como por las restantes normas desarrolladas al respecto.

Supuestos de adopción por la AEPD

- La AEPD podrá adoptar **cláusulas contractuales tipo** para la realización de transferencias internacionales de datos, que se someterán previamente al dictamen del Comité Europeo de Protección de Datos.
- Asimismo, la AEPD podrá aprobar **normas corporativas vinculantes**. El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de 1 año.

Supuestos de autorización previa de la AEPD

- Las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en ninguna garantía prevista en el GDPR requerirán una **previa autorización de la AEPD** o de las autoridades autonómicas (cuyo procedimientos durará un año), que podrá otorgarse en los siguientes supuestos:
  - Cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en **cláusulas contractuales que no correspondan a las cláusulas tipo** del GDPR.
  - Cuando la transferencia la lleve a cabo algún responsable o encargado de autoridades u organismos públicos y se funde en **disposiciones incorporadas a acuerdos internacionales no normativos** con otras autoridades de terceros Estados, siempre que incluyan derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento.

Supuestos de información previa

- Los responsables del tratamiento deberán informar a la AEPD, o en su caso, a las autoridades autonómicas de protección de datos, de cualquier transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con **intereses legítimos imperiosos** y sobre la **concurrencia del resto de requisitos previstos en el GDPR** (ej. el interesado ha dado su consentimiento explícito a la transferencia propuesta)[1].
- Esta información deberá facilitarse con **carácter previo** a la realización de la transferencia.

(1) Lo dispuesto no será de aplicación a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

Detalle
Autoridades de protección de datos

La AEPD y las autoridades autonómicas competentes son las autoridades de protección de datos recogidas en el PLOPD

Autoridades de protección de datos

Agencia Española de protección de datos

- La AEPD es una **autoridad administrativa independiente de ámbito estatal**, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones. Se relaciona con el Gobierno a través del **Ministerio de Justicia**.

Facultades y potestades

- Esta Agencia supervisará la **aplicación del GDPR** y del resto de normas relativas a la protección de datos, y ejercerá las funciones y potestades previstas en dicho Reglamento (ej. promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento).
- Además, la AEPD tiene encomendadas **potestades de investigación**, de elaboración de **planes de auditoría preventiva** referidos a los tratamientos de un sector concreto de actividad, de **regulación** (Circulares de la AEPD que serán obligatorias una vez publicadas en el BOE), y de **acción exterior del Estado** en materia de protección de datos, entre otras.

Autoridades autonómicas

- La autoridades autonómicas de protección de datos de carácter personal podrán ejercer las **funciones** y **las potestades** previstas en el GDPR cuando se refieran a:
  - **Tratamientos de los que sean responsables** las entidades integrantes de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial, o quienes les presten servicios a través de cualquier forma de gestión directa o indirecta.
  - Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de **funciones públicas** en materias que sean competencias de la correspondiente Administración Autonómica o Local.
  - Tratamientos que se encuentren expresamente previstos, en su caso, en los respectivos **Estatutos de Autonomía**.

Detalle

Procedimiento en caso de posible vulneración de la normativa

El procedimiento en caso de posible vulneración de la normativa de protección de datos se iniciará por la AEPD, la cual podrá acordar medidas provisionales necesarias y proporcionadas

Posible vulneración de la normativa de protección de datos

Régimen jurídico y clases de iniciación

- Las disposiciones serán de aplicación a los procedimientos tramitados por la AEPD en los supuestos en los que un **afectado reclame que no ha sido atendida su solicitud de ejercicio de los derechos** de las personas, así como en los que aquella investigue la existencia de una posible infracción.
- Los procedimientos regulados en este título se iniciarán por la Agencia Española de Protección de Datos por **propia iniciativa o previa reclamación**, una vez que ésta haya sido admitida a trámite[1] y se regirán por lo dispuesto en el GDPR y demás normativa aplicable.

Procedimiento

- **Admisión a trámite de las reclamaciones**. La AEPD deberá evaluar dicha admisibilidad a trámite (ej. no se admitirán reclamaciones cuando no versen sobre protección de datos de carácter personal o carezcan manifiestamente de un fundamento).
- **Actuaciones previas de investigación**. La AEPD podrá incoar actuaciones previas de investigación a fin de determinar si concurren circunstancias que lo justifiquen. El plazo máximo de tramitación será de 1 año.
- **Medidas provisionales**. La AEPD podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado. Cuando se considere que el tratamiento de los datos con carácter personal comporta un menoscabo grave con el derecho a la protección de datos, la AEPD podrá ordenar el bloqueo de los datos y la cesación de su tratamiento.

Plazo de tramitación

- Los plazos máximos de tramitación de los procedimientos y notificación de las resoluciones que los terminen se establecerán mediante Real Decreto, que no podrá fijar un plazo superior a **nueve meses**.
- Estos plazos **serán suspendidos** cuando deba recabarse información, consulta o pronunciamiento preceptivo de un órgano de la UE o de una autoridad de control conforme a lo dispuesto en el GDPR por el tiempo que medie entre la solicitud y la notificación del pronunciamiento.

(1) Con carácter previo, la AEPD determinará el carácter nacional o transfronterizo del procedimiento, además podrá incoar actuaciones previas de investigación para determinar si concurren circunstancias que lo justifiquen.

Detalle
Régimen sancionador

El PLOPD prevé un régimen sancionador aplicable a, entre otros, los responsables y encargados del tratamiento, y en el que se distingue entre infracciones muy graves, graves y leves, con multas y plazos de prescripción diferentes

Régimen sancionador

Sujetos responsables

- Estarán sujetos al régimen sancionador del GDPR y de la futura ley orgánica, entre otros, los responsables del tratamiento, encargados del tratamiento, representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la UE, etc[1].

Infracciones[2]

- Constituyen infracciones los actos y conductas que supongan la **vulneración de ciertas disposiciones del GDPR** relativas a las obligaciones de los sujetos responsables.

Infracciones muy graves

- Se considerarán muy graves y prescribirán a los **3 años** las infracciones que supongan una vulneración sustancial de lo previsto en el GDPR y en otros supuestos (ej. vulnerar los principios y garantías relativos al tratamiento previstos en el GDPR, incumplir las condiciones para el consentimiento del GDPR).

Infracciones graves

- Se considerarán graves y prescribirán a los **2 años** las infracciones que del mismo modo vulneren lo previsto en el GDPR y en otros supuestos (ej. el tratamiento de datos de carácter personal de un menor de 13 años sin su consentimiento, obstaculización reiterada de derechos).

Infracciones leves

- Se considerarán leves y prescribirán al **año** las restantes infracciones de carácter meramente formal de las previstas en el GDPR y en otros supuestos (ej. el incumplimiento del principio de transparencia de la información o el derecho de información del afectado).

Sanciones

- Las sanciones previstas en el GDPR se aplicarán considerando los **criterios de graduación** previstos (ej. naturaleza, gravedad y duración) y **otros criterios** como:
  - El carácter continuado de la infracción.
  - La vinculación de la actividad del infractor con tratamientos de datos de carácter personal.
  - Los beneficios obtenidos de la comisión de la infracción.
  - La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
  - Un proceso de función por absorción posterior a la infracción, no imputable a la entidad absorbente.

(1) Ver anexo para más detalle.
(2) Las categorías están recogidas en el GDPR. En concreto, los artículos 83.5 y 83.6 GDPR trata las infracciones muy graves, el 83.4 GDPR las graves y los artículos 83.4 y 83.5 GDPR las leves.

Índice

Próximos pasos

Una vez aprobada la nueva Ley Orgánica, ésta entrará en vigor el 25 de mayo de 2018, derogando la actual LOPD a partir de esa fecha

Próximos pasos

- La Ley Orgánica de Protección de Datos entregará en vigor el **25 de mayo de 2018**, fecha a partir de la cual quedará derogada la actual LOPD.

Índice

Anexo

Definición de responsable, encargado del tratamiento y representante

El GDPR recoge las definiciones de responsable y encargado del tratamiento así como del representante de estos, aplicables a efectos del PLOPD

Definiciones aplicables

Responsable del tratamiento

- De conformidad con el GDPR, por responsable de tratamiento o responsable se entenderá a la p**ersona 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 UE 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

- Según el GDPR, por encargado del tratamiento o encargado se entenderá a la **persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento**.

Representante

- De acuerdo con el GDPR, por representante se entenderá a la **persona física o jurídica establecida en la UE** que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento, **represente al responsable o al encargado** en lo que respecta a sus respectivas obligaciones en virtud del GDPR.