# Jornada concienciación sobre protección de datos

Víctor Seisdedos Potes | Director Dpto. Jurídico

# Índice

# Índice

# 1 | Introducción

# ¿Qué es un dato de carácter personal?

Un dato de carácter personal es toda información sobre una persona física identificada o identificable.

Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (artículo 4.1.a del RGPD).

Ejemplos prácticos:

- Nombre y apellidos.
- Domicilio.
- Dirección de correo electrónico.
- Número de teléfono.
- DNI o documento de identificación análogo, como ID o NIE.
- Datos de geolocalización.
- Dirección de Protocolo de Internet (IP)

# Índice

# 2 | Contexto normativo

# Fundamentos normativos (artículo 18 CE)

El derecho a la protección de datos, es un **derecho fundamental,** reconocido en nuestra Constitución Española (en adelante, CE) en el artículo 18.4 así como por nuestro Tribunal Constitucional (en adelante, TC), desde la STC 292 / 2000.

Se trata de un **derecho autónomo** (independiente de otros derechos).

Es un **derecho que tiene toda persona, sin importar la nacionalidad o la residenci**a, a la protección de los datos de carácter personal que la conciernan.

Por todo lo anterior, se comenzó a regular normativamente a través de diversos cuerpos legales.

# Contexto normativo

1992

## LORTAD

El primer cuerpo legal en España, fue la LORTAD (Ley Orgánica 5/1992 de 29 de Octubre, de regulación del tratamiento automatizado de datos de Carácter personal.

1999

## LOPD

Ley Orgánica 15/1999 del 13 de Diciembre de Datos de Carácter Personal (LOPD). Supuso la transposición de la Directiva 95/46, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

2007

## RLOPD

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD)

2016 - 2018

## RGPD

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)

2018

## LOPDGDD

Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales (LOPD – GDD)

# Actual normativa de protección de datos

El **RGPD** tiene como objetivo principal garantizar un **nivel uniforme de protección de las personas físicas**, estableciendo un mismo nivel de responsabilidad en todos los Estados miembros eliminando obstáculos de circulación de datos, proporcionando seguridad jurídica y transparencia a los operadores jurídicos.

Este cuerpo legislativo es aplicable (ámbito de aplicación material) tanto al **tratamiento automatizado** (soporte informático) **como al no automatizado** o manual (soporte papel). Sin embargo, quedan excluidas del RGPD:

- Las actividades domésticas o aquellas destinadas a la seguridad nacional.
- Datos de personas fallecidas (considerando 27 del RGPD).
- Datos anónimos, estadísticos o de investigación (Considerando 26 RGPD).

Una de las principales novedades del RGPD, es que es **aplicable** (ámbito de aplicación territorial) a **todos los países de la UE**, así como también es aplicable a todas las empresas extranjeras que ofrezcan productos o servicios de ciudadanos europeos .

# Índice

# 3 | Principios en materia de protección de datos

# Principios relativos al tratamiento (1 de 2)

**a) Principio de licitud, lealtad y transparencia**: los datos tienen que ser tratados de manera lícita, leal y transparente en relación con el interesado.

**b) Principio de limitación de la finalidad**: los datos tienen que ser recogidos siempre para un fin determinado, explícito y legítimo, y no pueden ser tratados posteriormente de manera incompatible con dicho fin.

**c) Principio de minimización de datos**: los datos tienen que ser adecuados, pertinentes y limitados a lo necesario en relación con el fin para el que son tratados.

**d) Principio de exactitud**: los datos tienen que ser exactos y, si fuera preciso, actualizados.

**e) Principio de exactitud**: los datos tienen que ser exactos y, si fuera preciso, actualizados.

# Principios relativos al tratamiento (2 de 2)

**f) Principio de limitación del plazo de conservación**: los datos tienen que ser mantenidos de tal manera que se permita la identificación de los interesados durante no más tiempo del necesario para el fin del tratamiento.

**g) Principio de integridad y confidencialidad**: se tienen que aplicar las medidas de seguridad, técnicas y organizativas apropiadas para garantizar la integridad y confidencialidad de los datos. El deber de confidencialidad persiste pese a que haya finalizado la relación contractual que nos obligaba al mismo.

**h) Principio de accountability o responsabilidad proactiva**: el responsable del tratamiento será responsable del cumplimiento de la normativa y de sus principios, así como de la capacidad de demostrarlo.

# Licitud del tratamiento (1 de 7)

Solo podremos tratar los datos de carácter personal de los interesados cuando tengamos una base legitimadora que lo habilite. Pero **¿Qué es una base legitimadora y cuántas hay?**

Una base legitimadora no es más que un **supuesto en el que el RGPD nos dice que podemos tratar los datos de carácter personal**. Existen seis bases legitimadoras.

La normativa en materia de protección de datos nos indica que debemos de saber qué base legitimadora habilita el tratamiento en cada momento. Sino la determinamos o no lo hacemos de la forma correcta, estamos incurriendo en un incumplimiento normativo.

# Licitud del tratamiento (2 de 7)

## Consentimiento del interesado

El consentimiento del interesado se tiene que entender como una **declaración o clara acción afirmativa**. Además, debemos tener en cuenta:

- Solo será de aplicación cuando ninguna de las otras bases de legitimación pueda ser aplicada.
- Tiene que ser expreso y estar diferenciado del resto de asuntos.
- Debemos tener capacidad de demostrar quien ha dado el consentimiento y para que finalidad. Para ello, no tendrán la condición de consentimiento las casillas pre-marcadas, oraciones en negativo o la inacción del interesado.
- Tiene que ser una declaración de voluntad libre, específica, informada e inequívoca.
- Puede ser retirado en cualquier momento. La forma de retirarlo debe de ser tan sencilla como la forma en que se dio.

# Licitud del tratamiento (3 de 7)

## Datos necesarios para la ejecución contractual o medidas precontractuales

Podemos tratar los datos de carácter personal de los interesados cuando sean necesarios para la ejecución de un contrato o para la aplicación de medidas precontractuales.

Por ejemplo:Vamos a realizar una reforma en nuestra vivienda, el contratista tendrá que tratar nuestros datos de carácter personal para realizar un presupuesto (medidas precontractuales). En el caso de que nos decantemos por ese contratista, a la hora de emitirnos la factura, tratará nuestros datos de carácter personal (son necesarios para la ejecución del contrato).

# Licitud del tratamiento (4 de 7)

## Cumplimiento de una obligación legal

Podemos tratar los datos de carácter personal de los interesados cuando sean necesarios para la ejecución de un contrato o para la aplicación de medidas precontractuales.

Podemos tratar los datos de carácter personal de los interesados cuando el responsable del tratamiento tenga que cumplir con una obligación legal.

Por ejemplo: La Ley de Universidades obliga que se realicen análisis de satisfacción y calidad de los servicios y productos. Los datos de carácter personal de los alumnos para la finalidad de analizar la satisfacción y calidad de los servicios y productos vienen determinados por la Ley, por tanto, se trata de dar cumplimiento a una obligación legal.

# Licitud del tratamiento (5 de 7)

## Intereses vitales

Podemos tratar los datos de carácter personal de los interesados en los casos en los que se necesite para proteger un interés esencial para la vida del interesado o de otra persona.

Por ejemplo: una persona de Barcelona acude de vacaciones a Zamora, se pone gravemente enfermo y acude al hospital. Para poder tratar su enfermedad y darle un diagnostico necesitan acceder a su historial médico.

# Licitud del tratamiento (6 de 7)

## Interés público o ejercicio de poderes públicos

Podemos tratar los datos de carácter personal de los interesados cuando sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. Por norma general, son facultades (no obligaciones) que le atribuye una Ley al responsable del tratamiento.

Por ejemplo: La Ley de Ciencia, Tecnología e Innovación habilita el tratamiento de datos de carácter personal con fines de investigación.

# Licitud del tratamiento (7 de 7)

## Interés legítimo

Podemos tratar los datos de carácter personal de los interesados cuando sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero. El interés legítimo no puede ser tratado como un cajón de sastre para todos los tratamientos que beneficien al responsable del tratamiento. Para poder utilizar como base legitimadora el interés legítimo, es necesario hacer un juicio de ponderación entre el interés legítimo del responsable del tratamiento y los derechos y libertades de una persona.

Por ejemplo: esta situación se da en la grabación de las llamadas por motivos de seguridad y calidad. El responsable del tratamiento debe de informar de que las grabaciones se van a llevar a cabo, pero no tiene por qué solicitar el consentimiento, tiene un interés legítimo en realizar dicho tratamiento. Ello se desprende del juicio de ponderación de derechos y libertades, primando la tutela judicial efectiva del responsable del tratamiento sobre la protección de datos de los interesados. O en el caso de que una empresa establezca cámaras de seguridad, tiene un interés legítimo en garantizar la seguridad de las personas, bienes e instalaciones.

# Principio de accountability

El principio de accountability responde a una cultura legislativa anglosajona, que a diferencia de la cultura continental, no tasa de manera específica cada una de las soluciones que se presentan ante un mismo problema.

Dicha diferencia la podemos ver con la anterior normativa en materia de protección de datos, la Ley Orgánica de Protección de Datos (en lo sucesivo LOPD), establecía una serie de medidas en función del riesgo al que se viera expuesta la empresa.

Actualmente, y siguiendo la influencia de la cultura de Compliance, el RGPD, lo que nos indica es que **corresponde a las empresas la responsabilidad de identificar los riesgos a los que se pueda ver expuesta la sociedad y, una vez identificados, seleccionar y aplicar las medidas** (técnicas, jurídicas y organizativas) adecuadas **para mitigarlo**.

Por ello es preciso crear políticas internas en materia de privacidad que garanticen y documenten todos los procesos de la empresa.

# Privacidad desde el diseño y por defecto

Para alcanzar los objetivo indicados, es necesario contar con dos conceptos clave:

**Privacidad desde el diseño**: se tienen que aplicar los mecanismos y **garantías necesarios desde el inicio de una actividad**, es decir, implica que desde el momento inicial del tratamiento de datos se tendrá que proceder a aplicar las medidas necesarias para garantizar la privacidad de los datos.

**Privacidad por defecto**: implica que se tendrán que aplicar medidas, por parte de la empresa, a **lo largo de la vida de los datos personales**, así como realizar tratamientos con los datos mínimos esenciales, esto es, implica que en todas las actividades se ejecuten protocolos que garanticen que solo se trataran los datos necesarios para desarrollar la finalidad para la que fueron recabados.

# Índice

# 4 | Refuerzo del manual de funciones y obligaciones del personal

Uno de los puntos fundamentales en el proceso de adecuación al RGPD de la sociedad es la de informar a todo el equipo de la empresa de su **Manual de Funciones y Obligaciones del Personal**. Por ello, se os ha hecho entrega de un Manual del personal, donde se describen las cuestiones relativas a la protección de datos.

Consideramos, como ejercicio de concienciación, destacar los puntos más relevantes de estos documentos con el fin de solventar cualquier tipo de duda que pudiera existir sobre los mismos:

- **El empleado deberá tratar toda información de carácter corporativo bajo la máxima confidencialidad,** es decir, que el empleado se obliga a utilizar la información única y exclusivamente con la finalidad de cumplir las funciones que tenga encomendadas, limitando el uso de dicha información para el desempeño de sus funciones.

- El empleado, debe implantar mecanismos para garantizar que la información manejada se **realiza de forma segura**.

En particular, el trabajador:

- N**o podrá divulgar dicha información** ni comunicarla a terceros, salvo el consentimiento por escrito de CAS TRAINING.

- **No obtendrá ninguna copia de la información para un uso personal**. Asimismo se debe evitar la realización de copias en local de la información recibida por parte del cliente para la realización de proyectos.

- Ante cualquier **riesgo o incidencia deberá comunicarlo a la empresa**, en particular, al Comité de Protección de Datos (véase más adelante)

- En el caso de rescisión del contrato laboral por alguna de las partes, el empleado **deberá devolver toda información independientemente** de su soporte (informatizado o papel), así como también la entrega de todo soporte.

- Asimismo, en el caso de tener alguna notificación en materia de protección de datos (de la Agencia Española de Protección de Datos, del propio cliente, etc.) o de terceros intervinientes (por ejemplo, una solicitud de derechos del interesado, es decir, ejercicio de derecho de acceso, rectificación, supresión, portabilidad, limitación del tratamiento) el empleado deberá notificárselo de forma inmediata al Comité de Protección de Datos.

# Índice

# 5 | Gestión y actuación práctica ante situaciones comprometidas por protección de datos


# Gestión de datos personales

Como ya se ha visto precedentemente, vosotros sois los que manejáis los datos de carácter personal de la compañía.

Por ello, sois vosotros los que deber tener la mayor cautela en poner la máxima precaución ante cualquier:

- **Brecha de seguridad** (lo veremos más adelante)
- **Ejercicio en materia de protección de datos** (también lo veremos más adelante)
- **Requerimiento** en materia de protección de datos.
- **Llamadas inusuales** (o amenazando) **sobre** cuestiones de protección de **datos**.
- Dar (o permitir) accesos indebidos a terceros de datos de carácter personal.

La máxima que debemos tener presente es tener siempre la **máxima transparencia** con las partes implicadas (bien sea internas o externas).


# Ejercicios de derechos

Como punto de partida, es importante destacar, que quienes ejercitan estos derechos lo pueden realizarán por cualquier medio (electrónico, burofax, etc.) pero **siempre mediará una solicitud**.

No obstante, la normativa de protección de datos exige que tengamos la certeza de la persona que ejercita el derecho (por ello en muchos casos se solicitaría fotocopia del DNI o documento equivalente).

Siempre que se tenga conocimiento del ejercicio de uno de los derechos que veremos a continuación obligatoriamente se le deberá responder (lo que proceda) en el plazo máximo de un (1) mes.

Un punto esencial a tener presente es que la muchas de sanciones emitidas por la Agencia Española de Protección de Datos, deriva de errores en el protocolo de contestación de ejercicio de derechos. Por ello, tal como hemos visto anteriormente, ante cualquier solicitud esta deberá ser derivada al Comité de Protección de Datos.


# Ejercicio de derechos

## Derecho de acceso

Este derecho reconoce al interesado la obtención **de que datos de carácter personal gestiona el responsable del tratamient**o, y en tal caso a la siguiente información:

- Finalidad del tratamiento
- Categoría del dato tratado
- Destinatarios de sus datos
- Plazo de conservación
- Existencia de otros derechos (rectificación, supresión, limitación y/u oposición)
- Reclamación ante la autoridad de control (AEPD)
- Origen de la fuente de obtención del dato
- Existencia de decisiones individuales automatizadas y/o elaboración de perfiles, así como la lógica aplicada para las mismas.
- Transferencias internacionales y garantías implantadas para la realización de las mismas.


# Ejercicio de derechos

## Derecho de rectificación

Supone la solicitud al responsable del tratamiento para **solicitar la modificación de datos ante tratamientos inexactos o incompletos de datos**. Este derecho viene reconocido en el artículo 16 y en el Considerando 65 del RGPD.


# Ejercicio de derechos

## Derecho de supresión

El Derecho de supresión de los datos, y que por tanto sean **suprimidos** por el responsable se da cuando:

- Deja de ser necesarios para los fines que fueron recogidos
- El consentimiento ha sido retirado por el interesado
- El interesado se opone al tratamiento (artículo 21 RGPD)
- Cuando hayan sido tratados ilícitamente
- Para dar cumplimiento a una obligación legal
- Los datos hayan sido obtenidos en relación con la oferta de servicios de la sociedad de la información.

En virtud de este derecho, en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.


# Ejercicio de derechos

## Derecho de supresión

Pero no todo ejercicio de derecho de supresión supone el borrado de datos, existe un bloqueo de datos personales ante una serie de supuestos:

- El ejercicio de las libertades de expresión o información.
- El cumplimiento de una obligación legal.
- Tratamiento para el cumplimiento de una misión realizada en interés público.
- Razones de interés público
- Fines de archivo en interés púbico, investigación, histórica o fines estadísticos.
- Formulación, ejercicio o defensa de reclamaciones.


# Ejercicio de derechos

## Derecho de limitación del tratamiento

Este derecho viene recogido en el artículo 18 y en el Considerando 67 del RGPD. Se trata de un marcado de datos de carácter personal conservados con el fin de limitar su tratamiento futuro. La limitación del tratamiento es un derecho en sí mismo, no dependiendo de otros derechos. Por ello el responsable deberá limitar el tratamiento ante:

- Impugnación de exactitud de datos.
- Tratamientos ilícitos en os que el interesado se opone a la supresión.
- Datos que ya no son necesarios para la finalidad del tratamiento, pero el interesado necesita para la formulación, ejercicio o defensa de sus reclamaciones.
- Ejercicio de derecho de oposición (artículo 21 RGPD).


# Ejercicio de derechos

## Derecho de portabilidad

El RGPD recoge este derecho en el artículo 20 y en el Considerando 68. Se trata de un derecho que tiene el interesado a recibir todos aquellos datos personales que le incumban y que haya facilitado a un responsable, basado en el consentimiento y dicho tratamiento se haya realizado mediante medios automatizados.

El responsable del tratamiento **deberá entregar dichos datos en un formato estructurado**, de uso común y lectura mecánica, pudiendo transmitirlos a otro responsable del tratamiento, siempre y cuando sea técnicamente posible.


# Ejercicio de derechos

## Derecho de oposición

En el artículo 21 y los Considerandos 69 a 70 desarrollan este derecho. El interesado podrá oponerse en cualquier momento a que datos personales que le conciernan sean objeto de un tratamiento. Como supuestos específicos se establecen:

- Tratamientos basados en datos en interés público (artículo 6.1.e del RGPD)
- Interés legítimo (artículo 6.1.f del RGPD)
- Ante servicios de sociedad de la información, el interesado podrá ejercitar su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

En caso de marketing directo (mercadotecnia directa), si el interesado se opone al tratamiento, el responsable está obligado a dejar de tratar dichos datos, incluida la elaboración de perfiles en la medida que esté relacionada con la citada mercadotenia.

A más tardar en el momento de la primera comunicación con el interesado, ha de presentarse al interesado de forma clara y al margen de cualquier otra información.


# Reporte brechas de seguridad

## Brecha de seguridad

Podemos entender como una brecha o violación de seguridad toda aquella pérdida, destrucción o alteración de datos de carácter personal, independientemente de la causa que los origine. Importante reforzar que las violaciones o brechas de seguridad tienen origen diverso (física, técnica, etc.)

Cualquier incidencia que detectéis, debéis indicarla a vuestro responsable directo, para que su vez se reporte al departamento informático así como a nosotros a efectos de analizar la incidencia detectada.

Ante esta situación, cuando se detecte un riesgo alto, tenemos la obligación de notificar dicha brecha ante la Agencia Española de Protección de Datos sin dilación indebida, a más tardar dentro de las primeras setenta y dos (72) horas desde que se produjo el incidente. Si la notificación se produce en un plazo mayor, se tendrá que justificar el motivo que lo ha originado.

A su vez, se tendrá que notificar la violación de seguridad al interesado cuando entrañe un alto riesgo para los derechos y libertades de las personas físicas.


# Reporte brechas de seguridad

Sin embargo sí es importante indicar que, como se ha visto anteriormente siempre será preciso comunicárselo al Comité de Protección de Datos, pero (lógicamente) también hay que indicárselo al supervisor inmediato así como al Responsable del Sistema Informático / IT.

La máxima que debemos tener presente es la plena desconfianza de todo (sin entrar en la paranoia). En muchas ocasiones las brechas de seguridad proceden por no prestar atención o confiar en la realización de las tareas diarias.

- Ejemplos de brechas / violaciones de seguridad:
- Robos físicos
- Pérdida de dispositivos (pendrive, disco duro, ordenador portátil, etc.) – 31% de los casos notificados ante la AEPD
- Ataque / virus en el equipo
- Revelación de datos a persona / destinatario erróneo
- Acceso indebido a información.
- Revelación de contraseñas de usuario
- Otros que podéis facilitar en el catálogo de brechas / violaciones de seguridad.


# Reporte brechas de seguridad

Tal como se ha indicado anteriormente, debemos (1) analizar la brecha de seguridad; (2) proceder a su registro y (3) en su caso, notificárselo a la Agencia Española de Protección de Datos (AEPD) y/o a los interesados.

Dicho proceso lo realizaríamos nosotros, pero en todos los casos precisamos de una información mínima:

- Volumen de datos afectados.
- Sujetos involucrados.
- Origen de la amenaza (qué y cómo ha sucedido).
- Datos que se han visto afectados.
- Todo lo anterior en cumplimiento de la “Política de notificación de brechas de seguridad” elaborada por la entidad.


# Medidas básicas de seguridad

- **Copias de seguridad**: de forma obligatoria todos los equipos deben trabajar contra el servidor para que la copia de seguridad pueda realizarse sobre la totalidad del mismo. Ahora bien, en el caso de que el empleado tuviere que realizar algún trabajo en su equipo local, será necesario, realizar una copia de seguridad de la información manejada (en particular sobre las bases de datos que contengan datos personales). Sin embargo, una vez finalice dicho acceso, deberá copiarse nuevamente en el servidor.

- **Contraseñas**: todos los equipos que se manejen a efectos internos deben contener contraseñas que impida el acceso a terceros. La AEPD establece que una contraseña es robusta, cuando tiene como mínimo ocho (8) caracteres, alfanumérica (alternancia de números y letras), siendo recomendable también la alternancia de mayúsculas y minúsculas con algún carácter especial (punto, coma, almohadilla, etc.)

- **Destrucción de documentación en papel:** toda información manejada en papel ha de estar correctamente custodiada y cuando ya no sea necesaria archivada. Asimismo, la documentación que no sea necesaria, ha de ser destruida a través de un mecanismo que garantice la destrucción íntegra del documento (por ejemplo, destructora de papel).


# Políticas de mesas limpias

- A colación de los puntos anteriores, es importante destacar que muchas información es manejada en soporte papel (cada vez menos), y un error / incumplimiento de este punto hace que suframos brechas de seguridad por esta vía.

- Pero toda la documentación que tengamos en soporte papel debe estar correctamente custodiada; y una vez finalizada la jornada laboral, correctamente archivada o destruida.

- Siempre hay que triturar la documentación en soporte papel, para garantizar que terceros no puedan acceder a dicha información.


# Comunicación datos a terceros

- **Encargados del tratamiento**: persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (artículo 4.1.8 del RGPD)

- **Cesión**: comunicación de datos a otro responsable del tratamiento para sus propias finalidades.

- **Transferencia internacional de datos**: 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 (los países de la Unión Europea más Liechtenstein, Islandia y Noruega).

# Índice

# 6 | Períodos generales de conservación de datos

- De acuerdo con los principios de calidad de los datos y minimización de datos, se establece la mínima conservación de los mismos, es decir, los datos tendrán que ser **cancelados o suprimidos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados**.

- En definitiva, una vez que se finalice un proyecto, toda información que se haya usado para el desarrollo del mismo, deberá ser eliminada, y en el caso de que el cliente nos lo solicite devolvérsela.

- Ahora bien, se podrán conservar los datos durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o, de la ejecución de un contrato o, de la aplicación de medidas precontractuales solicitadas por el interesado. Para ese supuesto la cancelación deberá producirse mediante el bloqueo de los datos, que sólo estarán a disposición de las Administraciones públicas, Jueces y Tribunales. Finalizado dicho plazo los datos deberán destruirse.

Los datos solo se conservarán durante el tiempo que sean necesarios. Pasado ese plazo de tiempo, si los datos están sujetos a una normativa específica, se deberán de bloquear hasta que se supere el plazo establecido, una vez superado se deberán destruir

Plazos de conservación más comunes según la normativa:

- **Documentación laboral, alta en la seguridad social y pago de las cuotas: 5 años** (Art. 21 del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social y art. 1964 del Código Civil).

- **Control de la jornada laboral: 4 años** (Art. 34.9 Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores).

- **Videovigilancia: 30 días** (Instrucción 1/2006, de 8 de noviembre, de la AEPD y art. 22.3 LOPDGDD).

- **Documentación contable y fiscal: 6 años** (Art. 30 Código Comercio).

- **Documentación contractual de empleados: 5 años** (Art. 1964.2 Código Civil (reformado por Ley 42/2015. De 5 de octubre).

# Índice

# 7 | Autoridad de control y sanciones

- La **autoridad de control en España**, es la Agencia Española de Protección de Datos (AEPD). Enlace: https://www.aepd.es/es

- Es la encargada de velar por el cumplimiento en España. Supervisa el cumplimiento en materia de protección de datos en los responsables y encargados del tratamiento. En su caso, realizará las inspecciones de cumplimiento, así como resolver las reclamaciones planteadas por personas físicas frente a las empresas jurídicas.

- **Sanciones**: de conformidad con la nueva normativa, evadir los preceptos legales del RGPD puede suponer **multas de hasta 20 millones de euros o 4% de la facturación global de la compañía.**

- **Criterios:**
  - la infracción cometida;
  - el volumen de negocio del infractor;
  - el grado de intencionalidad y negligencia en la infracción;
  - el grado de responsabilidad del Responsable y/o Encargado del Tratamiento;
  - si existe o no reincidencia;
  - categoría de datos personales y el volumen de datos que se ha visto expuesto;
  - si se ha notificado y colaborado con la autoridad de control;
  - la adhesión a Códigos de Conductas y
  - otros factores tales como beneficios obtenidos, pérdidas evitadas, etc.

# Índice

Como te hemos indicado en epígrafes anteriores, CAS TRAINING cuenta con un Responsable a efectos internos que sirve de punto de contacto entre nosotros y vuestra entidad.

Asimismo, para un cumplimiento riguroso de la normativa, de forma externa CAS TRAINING cuenta con nosotros como consultoría externa.

Si tuvieras cualquier duda o cuestión, le facilitamos a continuación los datos de contacto:

## Por parte de CAS TRAINING

D. Ignacio Álvarez Gallego | ignacio.alvarez@cas-training.com

## Por parte de ASTRA

D. Víctor Seisdedos Potes | legal@astralegalconsulting.com

# Contacto


DIRECCIÓN DE LA OFICINA PRINCIPAL

Paseo de la Castellana, 200 - 28046 Madrid

NÚMERO DE TELÉFONO

(+34) 912 519 404

CORREO ELECTRÓNICO

info@astralegalconsulting.com