RESUMEN LEGISLACIÓN PROTECCIÓN DATOS CARÁCTER PERSONAL (LOPD)

Resumen de obligaciones y sanciones

La Constitución Española establece en su artículo 18 el derecho a la intimidad de las personas cuando dice:

> *18.1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
>
> *18.4. La Ley limitará el uso de la Informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

El objeto de la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), que derogó la antigua LORTAD de 1992, es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, especialmente con la finalidad de preservar el honor, intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado. Todo esto es aplicable a los datos de carácter personal registrados en cualquier tipo de soporte físico susceptible de ser tratado (ya sea informático o manual).

Por lo tanto, con motivo de la entrada en vigor de la LOPD surgen una serie de obligaciones para aquellas Entidades Públicas o Privadas que posean ficheros con datos de carácter personal. Asimismo, el Reglamento de desarrollo de la LOPD (R.D. 1720/2007) establece la obligación para todas las organizaciones de poner en marcha diversas medidas destinadas a garantizar la protección de dichos datos, afectando a sistemas informáticos, locales, soportes de almacenamiento, personal, procedimientos operativos, etc.

Adicionalmente a esta legislación existen las Directivas de la Unión Europea, varios Reales Decretos que desarrollan la LOPD, así como diversas instrucciones publicadas en el BOE por la Agencia Española de Protección de Datos (AEPD). Las más importantes son:

- R.D. 428/1993: Estatuto de la Agencia Española de Protección de Datos.
- R.D. 195/2000: Plazos para implantar las medidas de seguridad.
- Sentencia Tribunal Constitucional del 30/11/2000, recurso 1563-2000, interpuesto por el Defensor del Pueblo contra los artículos 21.1, 24.1 y 2 de la LOPD 15/1999, BOE del 4/01/2001.
- Instrucción 1/1995, de 1 de marzo de la AEPD, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito.
- Instrucción 2/1995, de 4 de mayo, de la AEPD, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal.
- Instrucción 1/1996, de 1 de marzo de la AEPD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.
- Instrucción 1/1998, del 19 de enero, de la AEPD relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

Ver la web de la Agencia Española de Protección de Datos para mayor información: www.agpd.es

Obligaciones legales básicas de la normativa de protección de datos

- **Calidad de los datos**: Los datos de carácter personal sólo se podrán recoger para su tratamiento 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, no podrán usarse para otras finalidades incompatibles con aquellas, serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado y serán cancelados cuando hayan dejado de ser necesarios o pertinentes (Art. 4 LOPD).
- **Deber de secreto:** El Responsable del Fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero (Art. 10 LOPD).
- **Información en la recogida de datos**: Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, y de la identidad y dirección del responsable del tratamiento. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos estas advertencias en forma claramente legible (Art. 5 LOPD).
- **Consentimiento del afectado**: El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa. No será necesario dicho consentimiento cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas (Art. 6 LOPD), sean necesarios para un contrato o figuren en fuentes accesibles al público. Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Estos y los datos sobre origen racial, salud o vida sexual sólo podrán ser recogidos, tratados o cedidos, con el consentimiento expreso y por escrito del afectado. Sin embargo, estos tipos de datos sí podrán tratarse cuando resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario o equivalente, sujeto al secreto profesional (Art. 7 LOPD).

  Sin perjuicio de lo que se dispone en el artículo 11 de la LOPD respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad (Art. 8 LOPD).
- **Comunicación o cesión de datos**: Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del interesado. Sin embargo este consentimiento no será preciso cuando la cesión esté autorizada en una Ley, o cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica (cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros), o cuando los datos

procedan de fuentes accesibles al público, o cuando la cesión sea de datos relativos a la salud y sea necesaria para solucionar una urgencia (que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica), o cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos (Art. 11 LOPD).

- **Tratamiento por cuenta de terceros**: Deberá estar regulado en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el Encargado del Tratamiento únicamente tratará los datos conforme a las instrucciones del Responsable del Fichero, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad del RD 1720/2007 que el Encargado del Tratamiento está obligado a implementar.

  Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al Responsable del Fichero, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. En el caso de que el Encargado del Tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

- **Inscripción de los ficheros** en el Registro General de la Agencia Española de Protección de Datos (RGPD), en el caso de ficheros de titularidad pública con la previa publicación en Boletín Oficial de una Disposición General con la declaración de los ficheros (Artículos 20, 25 y 26 LOPD, y Título V del R.D. 1720/2007).
- Tutela del **derecho de los afectados de acceso, rectificación y cancelación**, estableciendo el procedimiento interno apropiado (Artículos 15 a 17 LOPD, y Título III del R.D. 1720/2007).
- **Redacción e implantación del documento de seguridad** que incluya toda la normativa de seguridad de índole técnica y organizativa necesaria para garantizar la seguridad de los datos objeto de tratamiento. Será de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información (Art. 9 LOPD y Título VIII, capítulo II, del RD 1720/2007).
- **Auditoría** cada dos años del cumplimiento de la legislación y de los procedimientos de seguridad (Artículos 96 y 110 del RD 1720/2007).

Resumen del reglamento de medidas de seguridad

El RD 1720/2007 (Reglamento de desarrollo de la LOPD 15/1999) establece las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros, centros de tratamiento, locales, equipos, sistemas, programas y personas que intervengan en el tratamiento de los datos de carácter personal sujetos al régimen de la LOPD.

El RD 1720/2007 identifica tres niveles de medidas de seguridad: BÁSICO, MEDIO y ALTO, los cuales deberán ser adoptados en función de los distintos tipos de datos personales de los que se disponga en cada fichero, según se expone en la tabla siguiente.

NIVEL	TIPO DE DATOS	MEDIDAS DE SEGURIDAD OBLIGATORIAS
BÁSICO	• Afecta a todos los ficheros o tratamientos de datos de carácter personal. • Ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual (cuando la única finalidad es realizar una transferencia dineraria a las entidades de las que los afectados sean asociados; o caso de ficheros que de forma accesoria contengan estos datos). • Grado de discapacidad o invalidez (salud) sólo para el cumplimiento de deberes públicos.	• Documento de seguridad • Régimen de funciones y obligaciones del personal • Registro de incidencias • Identificación y autenticación de usuarios • Control de acceso • Gestión de soportes • Copias de respaldo y recuperación, verificación semestral • Almacenamiento de ficheros no automatizados o en papel bajo llave • Pruebas sin datos reales
MEDIO	• Infracciones administrativas o penales. • Prestación de servicios de información sobre solvencia patrimonial y crédito. Cumplimiento o incumplimiento de obligaciones dinerarias. • Administraciones Tributarias. • Prestación de servicios financieros. • Entidades Gestoras y Servicios Comunes de la Seguridad Social, en el ejercicio de sus competencias en materia de recaudación. • Definición de las características o de la personalidad (evaluación del comportamiento).	• Medidas de seguridad de nivel básico • Responsable de Seguridad • Auditoría bienal • Medidas adicionales de Identificación y autenticación de usuarios (límite reintentos de acceso) • Control de acceso físico • Medidas adicionales de gestión de soportes (registro entrada y salida) • Registro de incidencias (anotación y autorización para los procedimientos de recuperación)
ALTO	• Ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. • Fines policiales sin consentimiento. • Actos de Violencia de género. • Operadores de servicios de comunicaciones electrónicas (datos de tráfico y de localización).	• Medidas de seguridad de nivel básico y medio • Seguridad en la distribución de soportes (cifrado) • Registro de accesos (tanto para ficheros automatizados como en soporte papel). • Medidas adicionales de copias de respaldo (copia en lugar diferente) • Cifrado de telecomunicaciones • Almacenamiento de ficheros no automatizados o en papel bajo llave y en áreas de acceso restringido

Infracciones LOPD

Se establecen una serie de sanciones a los Responsables de los ficheros que contengan datos de carácter personal. Estas se clasifican en leves, graves y muy graves, atendiendo a la infracción cometida.

LEVES

a) No atender la solicitud del interesado de rectificación o cancelación
b) No inscribir el fichero en el RGPD
c) No informar al afectado (según Art. 5 LOPD) al recoger sus datos
d) Incumplir el deber de secreto del Art. 10 LOPD

GRAVES

a) Crear fichero de titularidad pública o iniciar la recogida de datos sin que la correspondiente disposición general haya sido publicada en el Boletín oficial
b) Crear fichero de titularidad privada o iniciar la recogida de datos con finalidad distinta del objeto empresarial
c) Recoger datos sin el consentimiento expreso del afectado
d) Tratar o usar los datos conculcando principios de la LOPD o del RD 1720/2007
e) Impedir u obstaculizar ejercicio de los derechos de acceso y oposición
f) Mantener datos inexactos, o no rectificarlos o cancelarlos cuando afecte derechos de las personas
g) Vulnerar el deber de secreto sobre ficheros de nivel Medio
h) Mantener los ficheros, locales, programas o equipos incumpliendo las condiciones de seguridad del RD 1720/2007
i) No proporcionar a la AEPD cuantos documentos sean requeridos o obstruir la inspección
j) No inscribir el fichero en el RGPD, cuando haya sido requerido por la AEPD
k) No informar al afectado según los Art. 5, 28 y 29 LOPD, si han sido recabados de persona distinta del afectado

MUY GRAVES

a) Recoger datos en forma engañosa y fraudulenta
b) Comunicar o ceder datos, fuera de los casos en que esté permitido
c) Recabar y tratar datos especialmente protegidos sin consentimiento del afectado o excepción LOPD
d) No cesar el uso o tratamiento ilegítimo de datos tras requerimiento de la AEPD o del afectado
e) Transferencia temporal o definitiva de datos a países no homologados sin autorización de la AEPD
f) Tratar datos de forma ilegítima o con menosprecio de principios y garantías, cuando se impida o se atente el ejercicio de derechos fundamentales
g) Vulnerar el deber de secreto sobre datos especialmente protegidos o de nivel Alto
h) No atender u obstaculizar sistemáticamente el ejercicio de derechos de acceso, rectificación, cancelación y oposición
i) No atender sistemáticamente el deber de notificación al afectado de la inclusión en un fichero

Sanciones LOPD

La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas y a cualquier otra circunstancia que sea relevante para determinar el grado de incumplimiento de la legislación y de culpabilidad presentes en los hechos sancionados.

	SANCIONES a **entidades privadas**
LEVES	Multa de 601 € a 60.101 € (de 100.000 a 10 millones de Pts.)
GRAVES	Multa de 60.101 € a 300.506 € (de 10 a 50 millones de Pts.)
MUY GRAVES	Multa de 300.506 € a 601.012 € (de 50 a 100 millones de Pts)

Si el Responsable del tratamiento de los ficheros es una **Administración Pública**, el Director de la Agencia Española de Protección de Datos (AEPD) podrá proponer, si procedieran, la iniciación de actuaciones disciplinarias. El procedimiento y las sanciones serán las establecidas en la legislación sobre régimen disciplinarios de la Administraciones Públicas.

Adicionalmente, en el caso de utilización o cesión ilícita de datos que atenten contra los derechos fundamentales, el Director de la AEPD podrá requerir a los responsables de los ficheros, tanto públicos como privados, el cese de la utilización o cesión ilícita de los datos. Si se desatiende el requerimiento, se podrán inmovilizar los ficheros mediante resolución motivada.