



Protección de datos, puntos fundamentales



Índice

• La protección de datos de carácter personal	2
• Principios básicos	3
• Requisitos legales	4
• Cesión y transferencia de datos	5
• Infracciones y sanciones	6
• Glosario	7

La protección de datos de carácter personal

Introducción

La Ley Orgánica de Protección de Datos de Carácter Personal (L.O. 15/1999), de 13 de Diciembre desarrolla una serie de obligaciones para aquellas organizaciones que posean ficheros con datos de carácter personal.

Así mismo, desde el 26 de Junio de 1999 está en vigor el Reglamento de Seguridad (R.D. 994/1999 de 11 de junio) que desarrolla la mencionada Ley Orgánica y que establece la obligación de las organizaciones a poner en marcha diversas medidas destinadas a garantizar la protección de dichos datos, afectando a sistemas informáticos, archivos, soportes de almacenamiento, personal, procedimientos operativos, etc.

Por ello toda organización ha de adecuarse a esta normativa cumpliendo todas las exigencias legalmente establecidas.

Este documento pretende ser un breve acercamiento a la Ley, de tal forma que se perciban las líneas generales de la misma. La adaptación de los ficheros con datos personales a la ley dentro de las organizaciones requiere de un amplio conocimiento de la misma, así como de otras por las que se pudiera ver afectado dicha organización.

Legislación aplicable

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de Octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos.
- Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.
- Instrucciones de la Agencia de Protección de Datos.
- Real Decreto 1332/1994, de 20 de Junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

- Real Decreto 994/1999, de 11 de Junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Real Decreto 195/2000, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el Reglamento aprobado por el Real Decreto 994/1999, de 11-6-1999.

Ámbito de aplicación

La LOPD es aplicable a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Están excluidos de protección, los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.(e.g.: una agenda personal no es un fichero sometido a la aplicación de esta Ley).

Los ficheros sometidos a la normativa sobre protección de materias clasificadas, los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada se regirán además por la legislación específica en cada caso.



Principios básicos

Alcance de la legislación

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal cuando:

- Sea efectuado en territorio español en el marco de las actividades desarrolladas por del responsable del fichero.
- Si no está establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional Público.
- Cuando el responsable de fichero no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de los datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

Principios de protección de datos

Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho 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. Estos condicionantes han de ponerse en relación con el caso en concreto.

Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para la que los datos se hubieran recogido. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Los datos de carácter personal incorporados a un fichero han de responder a la situación actual, de manera que recojan todas las modificaciones surgidas, y una vez incorporadas responderán a la realidad y han de ser exactos, de manera que si resultan ser inexactos o incompletos, en todo o en parte, han de ser cancelados o sustituidos de oficio por el responsable del fichero.

Cuando se ha cumplido la finalidad para la que se recabaron los datos han de ser cancelados o destruidos, en caso de no ser posible han de ser bloqueados.

No serán conservados en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Se prohíbe la recogida de datos por medio de medios fraudulentos, desleales o ilícitos.

Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

- De que sus datos van a ser incluidos en un fichero, de la finalidad de la recogida y de los destinatarios de la información.
- De la obligatoriedad o no de dar esos datos.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante para que los afectados puedan ejercer sus derechos.

Todas estas advertencias deberán ser recogidas en aquellos cuestionarios e impresos utilizados para la recogida de los datos.

El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco, es decir, expreso o tácito, del afectado, salvo que la ley disponga otra cosa. Para los datos especialmente protegidos consentimiento expreso y por escrito dada la importancia de los mismos.

No será preciso el consentimiento, cuando los datos de carácter personal sean recogidos de fuentes accesibles al público, por las Administraciones Públicas, en las relaciones comerciales o contractuales, y en los puntos desarrollados en el art. 7.6 de la L.O. 15/99.

Requisitos legales

La seguridad de los datos

- El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.
- Los requerimientos de seguridad vienen desarrollados en el Real Decreto 994/1999, de 11 de junio, Reglamento de medidas de seguridad de los ficheros automatizados (y no automatizados) que contengan datos de carácter personal y que están sometidos al régimen de la LOPD.
- Tanto el responsable del fichero, como el encargado de tratamiento, así como cualquier persona que intervenga en cualquier fase del proceso, 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 o, en su caso, con el responsable del mismo.

Niveles de seguridad aplicables

Se establecen tres diferentes niveles de seguridad, atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información, clasificándolos según los tres siguientes tipos:

• Nivel básico

Ficheros que contengan datos de carácter personal.

• Nivel medio

Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos que permitan obtener la personalidad del individuo.

• Nivel alto

Ficheros que contengan datos especialmente protegidos y datos recabados para fines policiales.

Se consideran datos especialmente protegidos los relativos a la ideología, afiliación, religión y creencias, los que hagan referencia al origen racial, a la salud y a la vida sexual, así como los relativos a la comisión de infracciones penales o administrativas.

El responsable del fichero deberá elaborar e implantar la normativa de seguridad mediante un documento de obligado cumplimiento para el personal.

Los ficheros de nivel medio y alto están obligados, por ley, a una pasar una auditoria, interna o externa, bianual.

Registro de ficheros

Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos, así como todos aquellos cambios que se produzcan en la finalidad del fichero, en su responsable, en la ubicación, etc.

El interesado tendrá derecho a solicitar por escrito y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

La Disposición Adicional primera de la LOPD establece que los ficheros y tratamientos automatizados inscritos o no en el Registro de la Agencia de Protección de Datos deberán adecuarse a la L.O 15/99 dentro del plazo de 3 años, a contar de su entrada en vigor.

En el caso de los ficheros y tratamientos no automatizados el plazo establecido para su adecuación a la L.O. 15/99 es de 12 años, a contar desde el 24 de Octubre de 1995, fecha en que entró en vigor la Directiva 95/46/CE.



Cesión y transferencia de datos

Acceso a datos por cuenta de terceros

Se entiende por cesión de datos toda revelación de datos realizada a una persona distinta del interesado.

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. No será preciso el consentimiento:

- Cuando la cesión está autorizada en una ley.
- Cuando se trata de datos recogidos de fuentes accesibles al público.
- 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. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
- Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.
- Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- Cuando la cesión de datos de carácter personal relativos a la salud 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.
- Cuando los datos han sufrido un procedimiento de disociación no es necesario el consentimiento porque no son datos de carácter personal.

No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. Físicamente es una cesión de datos, sin embargo la Agencia de Protección de Datos no lo considera como tal, sino como

una prestación de servicios. Este tratamiento deberá estar regulado en un contrato escrito. El encargado de tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento y no los utilizará para fines distintos a los que figuren en el contrato. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento.

El encargado de tratamiento tendrá la misma responsabilidad que el responsable del fichero si los comunica o utiliza incumpliendo las estipulaciones del contrato.

Transferencias internacionales

Se define transferencia internacional de datos como el transporte de datos entre sistemas informáticos por cualquier medio de transporte, así como de datos por correo o por cualquier otro medio convencional.

No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen el nivel de protección que presta la LOPD.

La Orden de 2 de Febrero de 1995, del Ministerio de Justicia e Interior, establece la relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos.

La adecuación del nivel de protección que ofrece el país de destino lo evaluará la APD atendiendo a la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino, las normas de derecho vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

La transferencia de datos a países que no tengan un nivel de seguridad equivalente al español está prohibida, salvo que lo autorice el Director de la APD.

Infracciones y sanciones

Tipos de infracciones

El incumplimiento de la legislación vigente, en materia de protección de datos de carácter personal, conlleva la imposición de sanciones por parte de la Agencia de Protección de Datos.

Infracciones leves

▪ **Multa entre 601,01 € y 60.101,21 €**

- No solicitar la inscripción en la Agencia de Protección de Datos (APD)
- Recabar datos sin proporcionar la información previa exigida
- No atender las solicitudes de rectificación o cancelación
- No proporcionar información a la APD cuando sea requerida

Infracciones graves

▪ **Multa entre 60.101,21 € y 300.506, 05 €**

- No inscribir los ficheros a petición de la APD
- Crear ficheros con finalidades distintas a las de constitución
- Recabar datos de carácter personal sin la autorización del afectado
- Evitar el acceso a los ficheros
- Mantener datos inexactos o no efectuar las rectificaciones exigidas
- Tratar los datos violando los principios y garantías de la LOPD
- Tratar datos especialmente protegidos sin la autorización del afectado
- No remitir a la APD las notificaciones previstas en la LOPD
- Mantener ficheros sin las debidas condiciones de seguridad

Dentro de la propia Ley se especifican tanto el tipo de acción sancionable como los importes que pueden ser aplicados a las organizaciones que incumplan la ley.

Infracciones muy graves

▪ **Multa entre 300.506, 05 € y 601.012,1 €**

- Crear ficheros para almacenar datos que revelen datos especialmente protegidos
- Recogida de datos de forma engañosa o fraudulenta
- Recabar datos especialmente protegidos sin la autorización del afectado
- No atender u obstaculizar de forma sistemática las solicitudes de rectificación o cancelación
- Vulnerar el secreto sobre datos especialmente protegidos
- La comunicación o cesión de datos cuando no este autorizada
- No cesar en el uso ilegítimo a petición de la APD
- Tratar los datos de forma ilegítima o con menosprecio de principios y garantías que les sean de aplicación
- No atender de forma sistemática a los requerimientos de la APD
- Transferencia temporal o definitiva de datos de carácter personal con destino a países sin niveles de protección equiparables, o sin autorización



Glosario

- **Activo**

Recurso físico que permite dar soporte, almacenamiento, gestión o tratamiento de los ficheros, de forma directa o indirecta.

- **Afectado o interesado**

Persona física titular de los datos que sean objeto de tratamiento por parte de otros.

- **Análisis del riesgo**

Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información; para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

- **Auditoría**

Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el alcance al que se cumplen los procedimientos o requisitos contra los que se compara la evidencia.

- **Cesión de datos**

Toda revelación de datos realizada a una persona distinta del interesado

- **Consentimiento del interesado**

Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

- **Control de acceso**

Esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo mediante las contraseñas de acceso.

- **Datos de carácter personal**

Cualquier información concerniente a personas físicas identificadas o identificables.

- **Derecho de acceso**

Derecho del interesado a solicitar y obtener gratuitamente información de sus datos de carácter personal incluidos en ficheros sometidos a tratamiento, conocer el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

- **Derechos de cancelación y rectificación**

Facultad del afectado por la que puede instar al responsable del fichero a cumplir con la obligación de mantener la exactitud, complitud y adecuación de los datos. A tal efecto, puede solicitar del responsable la rectificación o, en su caso, la cancelación de los mismos.

- **Derecho de oposición**

En aquellos casos en los que no sea necesario el consentimiento del afectado para el tratamiento de sus datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal.

- **Documento de seguridad**

Documento en el que se detallan las características del Fichero con datos de carácter personal, el sistema de información que lo gestión así como todas las exigencias legales requeridas en función del nivel de seguridad exigido al mismo.

- **Encargado del tratamiento**

La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

- **Fichero**

Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

- **Medidas de seguridad**

Requerimientos exigidos a los ficheros con datos de carácter personal para que garanticen la seguridad de los datos en función del nivel de los mismos.

- **Nivel de seguridad**

Clasificación de los ficheros en función de los datos de carácter personal que posean.

- **Procedimiento de disociación**

Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable

- **Responsable de seguridad**

Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

- **Responsable del fichero o del tratamiento**

Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del fichero.

- **Seguridad**

Conjunto de medidas que tienen como objetivo garantizar la confidencialidad, integridad y disponibilidad de los sistemas de información.

- **Sistema de información**

Conjunto de ficheros, activos, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

- **Soportes**

Contenedores físicos que permiten almacenar de una forma u otra ficheros o datos de carácter personal.

- **Tratamiento de datos**

Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.



Aviso legal:

Los derechos de propiedad intelectual de todos los contenidos de este documento, su diseño gráfico y textos son titularidad de EFENET. Igualmente, todos los nombres comerciales, marcas o signos distintos de cualquier clase contenidos en este documento son propiedad de sus dueños y están protegidos por la ley. Por tanto, queda prohibida cualquier duplicación, reproducción, comunicación pública, transformación, uso de la información contenida, cualquier otra actividad que se pueda realizar con parte o la totalidad del presente documento o así como cualquier otra posible acción u omisión ni aún citando las fuentes, salvo consentimiento de EFENET.