Ley Orgánica de Protección de Datos

La ley de protección de datos de carácter personal (**LOPD**) es una ley orgánica que tiene como objetivo garantizar y proteger los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad y privacidad personal y familiar. Fue aprobada el 13 de diciembre del 1999.

Esta ley afecta a todos los datos que hacen referencia a personas físicas registradas sobre cualquier apoyo, **informático** o no. Quedan exentos del cumplimiento de esta normativa aquellos datos recogidos para uso doméstico, las materias clasificadas del estado y aquellos ficheros que recogen datos sobre terrorismo y otras formas de delincuencia organizada (no simple delincuencia).

A partir de esta ley se formó la Agencia Española de Protección de Datos.

Niveles de Protección de Datos

Los datos de carácter personal se estructuran en diferentes niveles que clasifican los registros en tres niveles de seguridad. Son datos de carácter personal:

- nombres y apellidos de personas físicas vivas
- números de DNI, NIF y pasaporte
- direcciones físicas que se asocien o se puedan asociar a través del tratamiento informático
- teléfonos y direcciones de correo electrónico que se asocien o se puedan asociar a través del tratamiento informático
- fotografías dónde se pueda reconocer claramente alguien
- voz a través de la cual se pueda reconocer alguien
- datos genéticos y médicas asociadas a personas concretas
- datos biométricos
- datos referidos a creencias, filiación política o sindical
- datos referidos a la raza
- cualquier dato que permita identificar alguien (la ley no opta por una enumeración cerrada, sino por la definición anteriormente expuesta; por lo tanto, la intención es otorgar el máximo de protección posible atendidos los continuos adelantos de la ciencia y la técnica)

Nivel básico

- Identificadores.
- Personal.
- Circunstancias sociales.
- Académicos y profesionales.
- Detalle de empleados.
- Información comercial
- Económico-financiero y de seguros
- Transacción

Nivel mediano

- Infracciones administrativas o penales.
- Hacienda pública.
- Servicios Financieros.
- Solvencia patrimonial y créditos.
- Evaluación de la personalidad.

Nivel alto

- Ideología.
- Creencias.
- Origen racial.
- Salud.
- Vida sexual.

Ámbito de Aplicación

La LOPD establece, en líneas generales, que la ley es aplicable a todas aquellas empresas y administraciones que den servicio a ciudadanos dentro del territorio español (Por ejemplo afectaría a una empresa que diera servicio a ciudadanos españoles desde cualquier lugar del mundo).

Por el contrario la ley no afecta a:

- Ficheros mantenidos por personas físicas en ejercicio exclusivamente personal o doméstico.
- Ficheros de materias clasificadas.
- Ficheros establecidos para la investigación de terrorismo y de delitos graves relacionados con la delincuencia organizada.
- Personas ya muertas.

Conceptos básicos

- **Dato Personal**: cualquier información del tipo que sea que permita identificar o haga identificable la persona física (no la persona jurídica).
- **Afectado**: persona identificada o identificable a quien corresponden las señas personales.
- **Fichero**: Todo conjunto organizado de datos de carácter personal, que permita acceso a los datos con criterios determinados, cualquiera que sea la forma o modalidad de creación, grabación, organización, tratamiento y acceso.
- **Responsable del fichero**: persona física o jurídica de naturaleza pública o privada a quien pertenezca el fichero, con independencia de que ejecute o no materialmente el tratamiento.
- **Sistema de Tratamiento**: cualquier forma o modalidad que permita el uso y gestión de los datos, desde que se registran hasta que se eliminan.
- **Encargado de Tratamiento**: puede ser el responsable del fichero o cualquier otra persona física o jurídica de naturaleza privada o pública que trate de encargo del responsable los datos de carácter personal de los ficheros. A la vez, este encargado de tratamiento puede

hacerlo solo o conjuntamente y en cada caso están todos los agentes implicados obligados a la normativa de confidencialidad desarrollada.

- **Usuario**: cualquier persona que tenga acceso a las señas personales que componen el o los fichero/s del responsable.
- **Responsable de Seguridad**: persona o personas físicas o jurídicas que tienen la función de velar por el cumplimiento, aplicación y mantenimiento del documento de seguridad.
- **Documento de seguridad**: recopilación de normativa y procesos para la aplicación de los aspectos regulados en materia de protección de datos que todo Responsable de Fichero debe tener obligatoriamente.
- **Comunicación de datos**: cualquier cesión de las señas personales del responsable del fichero a terceros. Toda comunicación o cesión de datos entre partes se debe dar en un marco regulado entre las partes de confidencialidad estricta y se deben garantizar la aplicación de las medidas de seguridad correspondientes así como que los datos serán tratadas para la finalidad con que fueron registradas, con la excepción de los requerimientos de determinadas administraciones públicas relacionadas con las funciones policiales, de justicia y sanidad.

Calidad del dato y niveles de seguridad

En función del nivel de datos registrados en el fichero con un u otro sistema de tratamiento, hará falta aplicar unas medidas de seguridad concretas que se desarrollan en el RDLOPD para cada uno de los niveles. Igualmente, el régimen sancionador es diferente en función de la calidad del dato implicado en la infracción. De forma que la normativa protege especialmente los datos cualificados como nivel alto, que tienen una especial relación con los derechos fundamentales de las personas.

Registro de ficheros

Todo responsable de fichero deberá registrar a La Agencia Española de Protección de Datos tantos ficheros como tenga identificados.

No tener los ficheros registrados es una primera infracción. Esto tiene numerosas implicaciones y obligaciones concretas para los responsables de fichero y a la vez supone una garantía mínima de calidad por la persona respecto de sus señas personales. El registro de ficheros es de acceso público y el que se comunica a la agencia es la identificación del fichero, el contenido de los datos (su calidad) así como la finalidad y cesiones que se hagan y la identificación de terceros implicados en la gestión y/o tratamiento de los datos. No se comunican los datos concretos, sino su composición para cada uno de los ficheros. Y se hace a través de la aplicación informática única que lo agencia dispone públicamente.

Consentimiento informado y derechos

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

1. 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.

2. Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

3. De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

4. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

5. De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Se permite sin embargo, el tratamiento de datos de carácter personal sin haber sido recabados directamente del afectado o interesado, aunque no se exime de la obligación de informar de forma expresa, precisa e inequívoca, por parte del responsable del fichero o su representante, dentro de los tres meses siguientes al inicio del tratamiento de los datos.

Excepción: No será necesaria la comunicación en tres meses de dicha información si los datos han sido recogidos de "fuentes accesibles al público" y se destinan a la actividad de publicidad o prospección comercial, en este caso "en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten".

Cláusula modelo

Esta podría ser una cláusula modelo de información/consentimiento de derechos amparados por la LOPD:

En cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD), (sustituir por el nombre del responsable del fichero), como responsable del fichero informa de las siguientes consideraciones:

Los datos de carácter personal que le solicitamos, quedarán incorporados a un fichero cuya finalidad es (describir la finalidad). Los campos marcados con asterisco (o cualquier otra señal) son de cumplimentación obligatoria, siendo imposible realizar la finalidad expresada si no aporta esos datos.

Queda igualmente informado de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, de sus datos personales en (sustituir por el domicilio para ejercitar los derechos).

Este es otro elemento capital de la legislación. En el momento que se recoja el dato de carácter personal el responsable del fichero debe hacerlo obteniendo el consentimiento informado del afectado. A la vez, ha de informar la persona afectada, como mínimo, de los siguientes aspectos:

- Identidad del Responsable del Fichero y advertencia de la existencia de fichero dónde serán registradas los datos.

- De los derechos que asisten el afectado respecto de sus señas personales: acceso, rectificación, cancelación y oposición.
- De la finalidad con qué son recogidas y de el uso que se dará, así como de posibles cesiones a terceros.

A la práctica, los responsables de fichero han optado por incluir cláusulas generales en formularios de recogida de las señas personales. Que en un u otro momento verifican que el afectado haya firmado o aceptado de forma explícita o tácita.

La ley también establece una serie de excepciones en las que no es necesario pedir consentimiento informado.

Consentimiento

Tipos de consentimiento

Consentimiento inequívoco

El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

Consentimiento tácito

Esta será la forma normal del consentimiento en los supuestos que no se exija un consentimiento expreso o expreso y por escrito.

Consentimiento expreso

Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

Consentimiento expreso y por escrito

Se requiere consentimiento expreso y por escrito del afectado respecto a los datos relativos a la ideología, afiliación sindical, religión y creencias y sólo podrán ser cedidos con consentimiento expreso.

Comunicación y cesión de señas personales a terceros

Otra obligación fundamental para el responsable del fichero la encontramos en la cesión y comunicación de datos. La cesión también debe tener el conocimiento y consentimiento del afectado y esto no siempre es así. Esta obligación adquiere especial relevancia en el contexto actual de subcontratación de servicios por las entidades.

De forma que podría ser que el dato fuese recogido por un responsable del fichero y que después fuera cedida a un tercero para un tratamiento específico. Por ejemplo, los datos de unos trabajadores pasados al servicio contratado de asesoría laboral, sin conocimiento ni consentimiento de los afectados, podrían ser posteriormente utilizadas por enviarlos publicidad comercial de servicios.

En cualquier comunicación o cesión de datos, para tratamiento o no, hay de haber un contrato entre el responsable del fichero y este tercer encargado del tratamiento donde se establezcan cuales son las finalidades del tratamiento y donde el encargado del tratamiento se comprometa a cumplir con la normativa vigente en materia de protección de datos. Resulta pues una garantía bastante importante para el afectado y en los procesos sancionadores de la Agencia Española encontramos importantes sanciones económicas por cesión ilegal de datos.

Confidencialidad del personal

Otra de las implicaciones normativas a tener muy presente y que es fundamental para el correcto tratamiento de las señas personales es la que se desprende del artículo 10 de la LOPD, que establece:*"El responsable del fichero y aquellos que 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 todavía tras finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."*

Resulta este otro de los artículos cuya vulneración centra una buena parte de los procesos sancionadores que instruye la agencia española. Pues implica una diversidad muy extensa de ámbitos y se una obligación general que recae sobre cualquier usuario que tenga acceso a los datos de cualquier fichero del responsable o encargado del tratamiento. Es la prueba de la responsabilidad al aplicar las medidas de seguridad al fichero no sólo por parte de la entidad responsable sino también por su personal y cargos, así como por los posibles encargados de tratamiento.

También en este caso los responsables del fichero han ido optando mayoritariamente por establecer cláusulas generales de obligación a la confidencialidad en los contratos laborales del personal, con colaboradores, terceros, etc.

Régimen sancionador

El régimen sancionador establecido por la legislación española es más estricto en comparación con otras de países vecinos. Dependerá en todo caso de la infracción cometida y especialmente de la calidad del dato implicado, pero el nivel económico de las sanciones se sitúa, en función del grado de la infracción, en:

- Sanción por **infracción leve**: de 601,01 € a 60.101,21 €
- Sanción por **infracción grave**: de 60.101,21 € a 300.506,05 €
- Sanción por **infracción muy grave**: de 300.506,05 € a 601.012,10 €

No obstando, el procedimiento sancionador no es el mismo para las entidades de derecho privado que para la administración pública. En caso de que sea la administración la que cometa una infracción el procedimiento pasará por una investigación que puede concluir con sanciones disciplinarias sobre el órgano y los cargos infractores, pero no con sanción económica. Tiene esto cierto sentido pues el dinero saldrían de la hacienda pública para ir a parar a la hacienda pública. Pero no hace falta pasar por alto que según la calificación de los datos que hace la propia ley, es precisamente la administración la que posee datos de mayor calidad: servicios sanitarios, educativos, tributarios, etc.. Por esta razón sería deseable que la normativa se adaptara de forma inmediata, por garantizar los derechos de los afectados.

Documento de Seguridad

Es el documento que todo responsable de fichero debe elaborar y disponer dónde se recoja el procesos que dan cumplimiento internamente a la normativa. Donde figure un responsable de seguridad, la identificación y registro de los ficheros, la normativa aplicable, el registro de usuarios, de apoyos, el inventario de sistemas de información y aplicaciones, y todo aquello relacionado con la implantación a la entidad de la normativa. Es un documento de garantía mínima de cumplimiento con las obligaciones derivadas de la normativa que toda entidad debería disponer, pero que por si mismo no implica el cumplimiento de las medidas de seguridad.