Unidad Didáctica 1

La protección de datos en las empresas

Contenido

1. La Protección de Datos

Vivimos en la sociedad de la información y cada día se tratan millones de datos personales.

Sin el uso de nuestra información personal prácticamente ninguno de los servicios de los que disponemos podría funcionar.

Hoy día, prácticamente para cualquier actividad, nos solicitan información. Facilitamos nuestros datos personales cuando abrimos una cuenta en el banco, cuando solicitamos participar en un concurso, cuando reservamos un vuelo o un hotel, cuando nos apuntamos al gimnasio, cuando pedimos hora para una consulta médica, cuando buscamos trabajo, cada vez que efectuamos un pago con la tarjeta de crédito o cuando navegamos por Internet.

El nombre y los apellidos, la fecha de nacimiento, la dirección postal o el correo electrónico, el número de teléfono, el DNI, la matrícula del coche y muchos otros datos que usamos a diario constituyen información valiosa que podría permitir identificar a una persona, ya sea directa o indirectamente.

También nuestros datos pueden ser recogidos en ficheros que dependen de las administraciones públicas y de empresas y organizaciones privadas que los utilizan para desarrollar su actividad.

Por tanto, nuestra información es importante, dice quienes somos, qué cosas nos gustan, cuáles son nuestras capacidades y habilidades. Nuestros datos, dicen todo sobre nuestra personalidad y es esencial al usarlos, saber cómo protegerlos.

Es habitual que prácticamente para cualquier actividad sea necesario que los datos personales se recojan y utilicen en la vida cotidiana.

Los mecanismos de recogida y tratamientos de los datos personales se encuentran en constante evolución.

Por esta razón, se ha de destacar la enorme importancia que en los últimos años está teniendo la Protección de Datos de Carácter Personal en todos

los ámbitos y tras la reciente entrada en vigor del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La protección de datos tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal, de posibles malos usos. Por lo tanto el derecho fundamental a la protección de datos, es la capacidad que tiene el ciudadano para disponer y decidir sobre todas las informaciones que se refieran a él. Es un derecho reconocido en la Constitución Española, en el Derecho Europeo y protegido por la Ley Orgánica de Protección de Datos (LOPD).

De este modo, la Ley Orgánica de Protección de Datos de Carácter Personal 15/1999, de 13 de Diciembre (LOPD) y las demás normas aplicables, imponen una serie de medidas de carácter técnico, organizativo y jurídico a aquellos que posean datos de carácter personal. (empresas, organismos públicos...), para evitar un mal uso o un uso inadecuado de los datos de carácter personal y evitar que se vulneren derechos fundamentales.

La Ley Orgánica 15/1999 regula el derecho fundamental a la protección de datos y dispone que será la Agencia Española de Protección de Datos la encargada de tutelar y garantizar el derecho.

Recuerde

Toda persona física tiene derecho a la protección de los datos de carácter personal que le conciernen y este derecho le atribuye la facultad de controlar sus datos.

Este manual tiene por objeto ayudarnos a saber cómo debemos actuar cuando alguien ha solicitado o utilizado nuestros datos personales y a defender

nuestros derechos pero también a aprender a comportarnos adecuadamente cuando usamos datos de los demás. En nuestra sociedad, adquirir una cultura sobre protección de datos es básico para la convivencia.

2. ¿A quién afecta la Ley Orgánica de Protección de Datos?

Cualquier entidad de carácter público o privado está obligada a cumplir toda la normativa en vigor relativa a protección de información personal amparada por la LOPD. La protección de los datos de las personas es un derecho fundamental que la Ley tiene por misión garantizar.

Las Administraciones Públicas, en el ejercicio de su actividad, están plenamente sometidas al cumplimiento de la normativa.

En el caso de entidades mercantiles, desde trabajadores autónomos hasta grandes corporaciones o grupos, sea cual sea la personalidad jurídica que adopten, todas ellas recaban en la práctica datos de carácter personal que suelen incorporar en ficheros, ya sean estos en papel o informatizados. Por ello están sujetas a la Ley en la medida en que traten datos de carácter personal sobre personas físicas cualesquiera (clientes, proveedores, empleados), a fin de salvaguardar el derecho a la propia intimidad de las personas.

La legislación sobre Protección de Datos marca una serie de límites a la utilización de los datos personales afectando a todas las empresas de nuestro país, ya que en mayor o menor medida todas tratan o manejan datos de carácter personal de personas físicas.

No obstante existen excepciones a las obligaciones fijadas por la LOPD. Según su artículo 2.2 la LOPD no será de aplicación:

- A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
- A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Por otra parte, según lo dispuesto por el artículo 2.3 de la LOPD determinados tratamientos se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por la LOPD. Se trata de los ficheros regulados por la legislación de régimen electoral; los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública; los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas; los derivados del Registro Civil y del Registro Central de Penados y Rebeldes; los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

3. ¿En qué consiste la protección de datos?

Todas las empresas y empresarios están obligados por ley a declarar y registrar los datos de personas físicas que utilizan en su actividad comercial. Este manejo y obtención de datos hace necesaria su adecuación a la vigente ley de protección de datos, que obliga a estas a organizar y proteger esta información, adoptando las medidas de índole técnico y organizativo necesarias que garanticen la seguridad de los datos.

Para garantizar el cumplimiento de dichas medidas, debemos poner en práctica las obligaciones que se derivan de la LOPD, y que son las citadas a continuación.

3.1. Creación e Inscripción de los ficheros en la Agencia Española de Protección de Datos

Para la creación e inscripción de los ficheros en la agencia española de protección de datos se deben seguir los siguientes pasos:

- Creación de los ficheros en función de la naturaleza de los datos de carácter personal de los que dispongamos, (entendiendo por fichero, todo conjunto organizado de datos de carácter personal). Ej: Fichero personal, el cual contiene datos del personal de la empresa como: nombres, apellidos, direcciones, nº de la Seguridad Social…
- Inscripción de ficheros.
  Una vez realizada la creación de los ficheros, es obligatorio inscribir los ficheros de datos de carácter personal en el Registro General de la Agencia Española de Protección de Datos.
  La inscripción la debe realizar el responsable del fichero con anterioridad al uso de los ficheros, cuando se producen cambios con respecto a la inscripción (Modificación de la estructura o características de sus bases de datos…), o cuando cesa el uso del fichero. (Debe darse de baja el fichero en la AGPD).
  La notificación de los ficheros a la agencia española de protección de datos implica el compromiso por parte del responsable de que el fichero declarado para su inscripción cumple con todas las exigencias legales.
  La inscripción de los ficheros no supone ningún coste y permite que los titulares de los datos puedan conocer quienes son los responsables de los ficheros ante los que ejercitar directamente los derechos de acceso, rectificación, cancelación y oposición.

Recuerde

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

3.2. Información al interesado, como titular de sus datos, de la existencia del fichero y su finalidad y la obtención del consentimiento de los interesados

Este deber se refiere al derecho que tiene el sujeto, cuyos datos personales han sido recabados de ser informados "de modo expreso", preciso e inequívoco de que dichos datos se incorporarán a un fichero o tratamiento de la empresa, además se le informará de la finalidad que tiene el mismo.

Otras de las principales obligaciones, consiste en obtener el consentimiento, en los supuestos establecidos por la LOPD de aquellos, de quienes se recaban los datos de carácter personal.

Recuerde

La ley reconoce a toda persona el derecho a saber por qué, para qué y cómo van a ser tratados sus datos personales y a decidir acerca de su uso.

3.3. Informar al interesado, de los derechos de los que disponen para hacer valer ante la empresa. Los Derechos Arco

A través de los derechos de acceso, rectificación, cancelación y oposición, también conocidos como derechos ARCO, podemos saber qué información per-

sonal se está tratando por un responsable, de quién o de dónde se obtuvieron los datos y a quién se los ha cedido, modificar o rectificar errores, cancelar datos que no se deberían estar tratando u oponernos.

Estos derechos los podemos definir de la siguiente manera:

- **Derecho de acceso**
  El derecho de acceso es la facultad de todo interesado de solicitar y obtener información acerca de sus datos de carácter personal que estén sometidos a tratamiento, el origen de dichos datos y las comunicaciones realizadas o que se prevean hacer de los mismos.
- **Derecho de cancelación**
  La cancelación es el proceso de borrado de datos que se debe realizar en los supuestos en que los datos del fichero resulten inadecuados o excesivos con relación a su finalidad, así como cuando dejen de ser necesarios para el fin para el que fueron recabados.
- **Derecho de rectificación**
  La rectificación es un proceso a aplicar en aquellos supuestos en los que existan datos erróneos o inexactos en los ficheros. A diferencia de la cancelación, no consiste en el borrado o destrucción física de los datos, sino únicamente en la sustitución de los mismos por aquellos que sean correctos.
- **Derecho de oposición**
  La oposición implica la negativa del interesado a que sus datos sean utilizados con determinada finalidad, entre las varias para las que fueron entregados.
  Dicha petición implicará que los datos personales podrán usarse para los fines permitidos pero no podrán utilizarse con las finalidades que el interesado no desee.

3.4. Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos

El RDLOPD obliga a adoptar unas medidas de seguridad con el fin de proteger los datos de carácter personal contenidos en los ficheros, tanto automatizados (informáticos) como no automatizados (papel o manual). El responsable

que trata datos personales debe garantizar su seguridad y para ello debe disponer de políticas de seguridad que permitan garantizar la integridad, disponibilidad y confidencialidad de los datos.

El RDLOPD distingue tres niveles de seguridad (Básico, Medio, y Alto), en función de la naturaleza de la información de carácter personal tratada.

Mencionamos a continuación algunas de las medidas que se pueden adoptar en materia de protección de datos en las empresas:

- Definir las funciones y obligaciones de los usuarios con acceso a datos de carácter personal, como de toda aquella persona que preste servicios en la empresa, para evitar su tratamiento o utilización por terceras personas que no estén autorizadas para ello.
- Establecer procedimientos de notificación, gestión y respuesta ante las incidencias, es decir, debemos reflejar las infracciones de cualquier medida de seguridad por cualquier usuario o por persona que preste servicios en la empresa para tomar las medidas oportunas para evitar que vuelva a ocurrir en el futuro e imponer sanciones disciplinarias.
  ¿Qué se entiende por incidencia?
  Incidencia es cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, tales como pérdida o deterioro de datos en cualquier soporte físico o automatizado que pudiera contener datos de carácter personal.
  El usuario o cualquier persona que detecte cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, debe notificar al Responsable del fichero o al Responsable de Seguridad de forma inmediata de la incidencia advertida, para que este último proceda al análisis de las incidencias ocurridas. Como consecuencia de este análisis, el responsable del fichero o el responsable de Seguridad determinarán las acciones inmediatas a tomar, la resolución de la misma y la toma de acciones correctivas para evitar que dichos hechos puedan volver a suceder y poner en peligro la protección de datos almacenados para su tratamiento.
  El responsable del Fichero o de Seguridad deberá de registrar:

  - El tipo de incidencia.
  - Fecha y hora en que se produjo o se detecta.
  - Persona que realiza la notificación.

- Persona a quien se comunica.
- Efectos que puede producir la incidencia.
- Descripción detallada de la misma.
- Medidas correctoras aplicadas.

- El Responsable del Fichero o el responsable de Seguridad deberá establecer el procedimiento de control de Accesos a los Ficheros o Tratamientos de datos de carácter personal, así como una relación de usuarios autorizados para acceder a los mismos, y establecer mecanismos que eviten el acceso no permitido. Se establecerán las mismas condiciones para el personal ajeno.
- Establecer criterios de almacenamiento de los datos de carácter personal para su protección, como:

  - Cerrar con llave las áreas o zonas que contengan datos de carácter personal, para evitar el acceso a personas no autorizadas.
  - Guardar en armarios con llave, la documentación que se encuentra en ficheros manuales (soporte papel).
  - La asignación de claves para poder acceder a los ficheros automatizados.

3.5. Creación de un Documento de Seguridad, de obligado cumplimiento para el personal con acceso a los datos de carácter personal, y a los sistemas de información

Se deberá elaborar el Documento de Seguridad al que obliga la normativa vigente, donde se contemplen las medidas de seguridad, técnicas y organizativas, previstas para proteger la información de carácter personal contenida en los ficheros o tratamientos de la empresa.

El RDLOPD establece la necesidad no solamente de redactar el Documento de Seguridad, sino también de mantenerlo actualizado, conforme a las variaciones experimentadas en el sistema de información o tratamiento de los datos de carácter personal.

Nota

El documento de seguridad, es de carácter privado y de obligado cumplimiento. No ha de enviarse a la Agencia Española de Protección de Datos, debe permanecer en la empresa. Nos lo pedirán en caso de Inspección para comprobar que se adoptan las medidas necesarias para proteger la información de carácter personal contenida en los ficheros o tratamientos de nuestra empresa.

3.6. Información al personal de las normas de seguridad y consecuencias de su incumplimiento

Es obligación del Responsable del Fichero o Tratamiento, informar, definir y documentar las funciones y obligaciones de los usuarios o perfiles de usuarios con acceso a datos de carácter personal y a los sistemas de información.

El Responsable debe formar y concienciar a los diversos intervinientes en el tratamiento de datos, es decir, debe formar a los usuarios del sistema de la información acerca de las obligaciones que han de atender para el cumplimiento de la normativa de protección de datos, mediante la entrega de los correspondientes manuales.

Formar al Responsable de Seguridad designado por el Responsable del Fichero, (en ficheros de nivel medio y alto) como encargado de coordinar y controlar el correcto cumplimiento de las medidas establecidas en el Documento de Seguridad.

El incumplimiento de esta obligación por parte del personal puede constituir un delito de revelación de secretos que daria lugar a la comisión de una Infracción Grave sancionada con una multa de 40.001 a 300.000 €.

3.7. Deber de secreto

El secreto es esencial para garantizar el derecho fundamental a la protección de datos. Sin secreto sobre los datos sobre los que se conozca no existiría este derecho.

La LOPD señala en su artículo 10 que;

> *"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 aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".*

El deber de secreto incumbe tanto al empresario como al personal a su servicio. Por ello, es conveniente que los empleados firmen una cláusula de confidencialidad.

Ejemplo

Que en determinados servicios de atención telefónica se realicen preguntas para establecer la identidad del cliente antes de facilitar datos, que en un hospital nunca nos faciliten información sobre una persona que esté siendo atendida, o que nunca nos den acceso a datos de personas mayores de edad, aunque se trate de familiares directos, si no aportamos un escrito probando que nos han otorgado su representación.

3.8. Acceso a datos por cuenta de terceros

En el desarrollo de la actividad de una empresa suelen existir terceras personas o empresas que prestan servicios a la misma y que, para ello, tienen acceso a los datos de carácter personal.

Los tratamientos de datos de carácter personal por cuenta de terceros deben estar regulados en un contrato escrito.

Conforme al artículo 12 de la LOPD, se redactarán los contratos de acceso a datos por terceros, tales como las asesorías laborales, contable/fiscal o empresas de mantenimiento informático, tanto de equipos como de aplicaciones.

En el caso de que un tercero preste servicio sin acceso a datos (servicios de limpieza, vigilancia, mantenimiento de instalaciones, etc.), se articulará el modo de recoger expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los mismos, que el personal hubiera podido conocer, con motivo de la prestación del servicio.

3.9. Prohibición de comunicar o ceder los datos personales a un tercero sin consentimiento previo del interesado (por ej.: para envíos publicitarios u ofertas de terceros)

La cesión de datos es "toda revelación de datos realizada por persona distinta del interesado". Este concepto es muy amplio, puesto que revelación recoge tanto la entrega, comunicación, consulta, interconexión, transferencia, difusión o cualquier otra forma que facilite el acceso a los datos de un fichero a un tercero, distinto del interesado.

La Ley Orgánica de Protección de Datos de Carácter Personal establece que solo será posible la cesión de los datos para el cumplimiento de los fines para los que fueron obtenidos y para otras funciones previa información y consentimiento del interesado. Lo que se pretende es evitar que se realicen cesiones por cualquier motivo, caprichosas, superficiales o que tengan poco o nada que ver con el ámbito de las funciones, atribuciones o competencias de la empresa cedente y la empresa cesionaria.

Recuerde

Si el interesado no da su consentimiento no se podrán ceder sus datos a un tercero.

En resumen, la protección consiste en la aplicación de una serie de medidas:

OLBIGACIONES QUE SE DERIVAN DE LA LOPD
Creación e inscripción de los ficheros en la Agencia Española de protección de Datos.
Información al interesado, como titular de sus datos, de la existencia del fichero y su finalidad y la obtención del consentimiento de los interesados.
Informar al interesado, de los derechos de los que disponen para hacer valer ante la empresa.
Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos.
Creación del Documento de Seguridad, de obligado cumplimiento para el personal con acceso a los datos de carácter personal y a los sistemas de información.
Información al personal de las normas de seguridad y consecuencias de su incumplimiento.
Deber de secreto.
Acceso a datos por cuenta de terceros.
Prohibición de comunicar o ceder los datos personales a un tercero sin consentimiento previo del interesado (por ej: para envíos publicitarios u ofertas de terceros).

4. Nivel de Protección

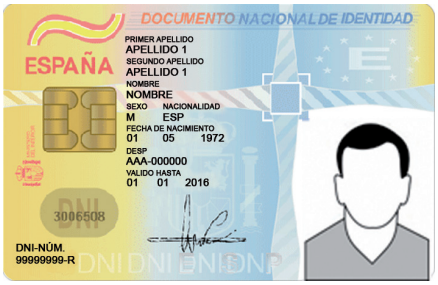
Existen diferentes niveles de seguridad, que determinarán una mayor o menor protección de los datos, estos niveles se establecen según la naturaleza de los datos, de tal forma que los podemos clasificar en los siguientes niveles:

4.1. Nivel Básico

La mayoría de datos de carácter personal son considerados de nivel básico. Pueden clasificarse en diferentes grupos:

Datos de carácter identificador

DNI/NIF, número de la Seguridad Social/mutualidad, nombre y apellidos, dirección postal y electrónica, teléfono, firma/huella digitalizada, imagen/voz, marcas físicas, firma electrónica.



Datos de características personales

Datos de estado civil, de familia, fecha y lugar de nacimiento, edad, sexo, nacionalidad, lengua materna, características físicas o antropométricas.

Datos de circunstancias sociales

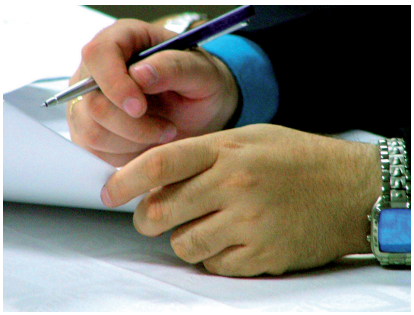
Características de alojamiento, vivienda, situación militar, propiedades, posesiones, aficiones y estilos de vida, pertenencia a clubes, asociaciones, licencias, permisos, autorizaciones.

Datos académicos y profesionales

Formación, titulaciones, historial de estudiante, experiencia profesional, pertenencia a colegios o a asociaciones profesionales.

Datos de detalles de empleo

Profesión, puestos de trabajo, datos no económicos de nómina, historial del trabajador.



Datos de información comercial

Actividades y negocios, licencias comerciales, suscripciones a publicaciones/ medios de comunicación, creaciones artísticas, literarias, científicas o técnicas.

Datos económicos-financieros y de seguros

Ingresos, rentas, inversiones, bienes patrimoniales, créditos, préstamos, avales, datos bancarios, tarjetas de crédito, planes de pensiones, jubilación, datos económicos de nómina, datos de deducciones impositivas/impuestos, hipotecas, subsidios, beneficios, historial de créditos.

Datos de transacciones de bienes y Servicios

Bienes y servicios suministrados por el afectado, bienes y servicios recibidos por el afectado, transacciones financieras, compensaciones/ indemnizaciones.

4.2. Nivel Medio

Datos relativos a la comisión de infracciones administrativas o penales.

NOTIFICAR A: Nombre Apellido Apellido

JUZGADO DE INSTRUCCIÓN Nº1 DE SEVILLA
Av Menendez Pelao
Teléfono:
Procedimiento: DILIGS. PREVIAS 2342/2008. Negocio: Z
N.I.G.: 12342P1345356356
Ejecutoria:
De: Nombre Apellido Apellido
Procurador/a:
Letrado/a:
Contra:
Procurador/a:
Letrado/a:

Auto

En Sevilla a catorce de enero de dos mil ocho

Hechos

Único.- El presente procedimiento se inición por los hechos que resultan de las anteriores actuaciones, habiéndose practicado las diligencias de investigación que constan en autos.

Rezonamientos Jurídicos

Primero.- De lo actuado se desprende que los hechos investigados son constitutivos de infracción penal, si bien aunque existen motivos suficientes para atribuir su perpetración a persona alguna determinada sin embargo, la misma tiene su domicilio fuera del territorio nacional y por ello es procedente, de conformidad con lo dispuesto en

Hacienda Pública, servicios financieros, solvencia patrimonial o crédito.

Datos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

Seguros Universal

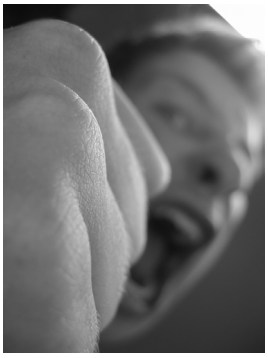
El conjunto de datos que permitan obtener una evaluación de la personalidad o aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social.

4.3. Nivel Alto

Ideología u opciones políticas, afiliación sindical, religión o creencias, origen racial, salud y vida sexual.

Datos recabados para fines policiales sin consentimiento de las personas afectadas.

Datos derivados de actos de violencia de género.



Nota

En los ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.
- Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.
- Se traten de datos relativos a la salud, referentes exclusivamente al grado de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

5. Datos especialmente protegidos

Los datos especialmente protegidos, también conocidos como *"datos sensibles"* son una categoría de datos que por su especial influencia en la intimidad, derechos fundamentales y las libertades públicas del individuo, requieren de una mayor protección que el resto de sus datos personales. Su tratamiento se encuentra regulado en el artículo 7 de la LOPD y son los siguientes:

- Datos que revelen la ideología, afiliación sindical, religión y creencias.
- Datos que hagan referencia al origen racial, la salud o la vida sexual.
- Datos relativos a la comisión de infracciones penales o administrativas.

El responsable del fichero debe tratar los datos especialmente protegidos en las condiciones previstas en el artículo 7 de la LOPD, dichas condiciones son las siguientes:

- **Derecho a no declarar sobre la ideología, afiliación sindical, religión o creencias.**
  De acuerdo con lo establecido en el artículo 16.2 de la Constitución Española, nadie podrá ser obligado a declarar sobre su ideología, afiliación sindical, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento para el tratamiento de dichos datos, se advertirá al interesado acerca de su derecho a no prestarlo. (Artículo 7.1 de la LOPD).
- **Tratamiento de los datos que revelen ideología, afiliación sindical, religión o creencias.**
  El tratamiento de estos datos solo podrá realizarse con el consentimiento expreso y por escrito del interesado. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de la cesión de dichos datos precisará siempre el previo consentimiento del afectado (art.7.2 de la LOPD).
- **Tratamiento de los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual.**

Este tipo de datos solo podrá ser recabado, tratado y cedido cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente (art.7.3 de la LOPD).

Ejemplo: Datos de origen racial sería el color de la piel, raza concreta a la que pertenece el sujeto; datos de salud como enfermedades padecidas, análisis clínicos, radiografías, etc.; datos de vida sexual, como hábitos sexuales, prácticas de riesgo, uso de anticonceptivos, etc.

- **Tratamiento de los datos de carácter personal relativos a la comisión de infracciones penales o administrativas.**

  Este tipo de datos solo podrá ser incluido en los ficheros de las administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

  La LOPD entiende que se deben proteger estos datos, porque si se vulneran los tratamientos de los expedientes sancionadores se puede atentar gravemente al derecho a la intimidad (art.7.5 de la LOPD).

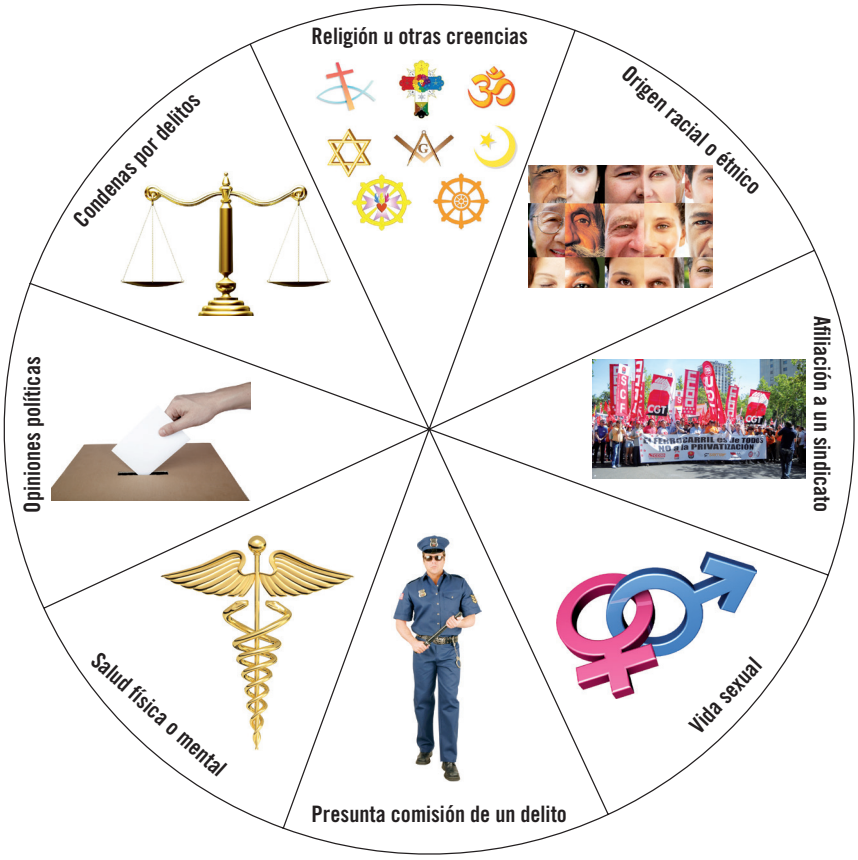
- **Ficheros prohibidos.**

  Debemos mencionar que quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual (artículo 7.4 de la LOPD).

- **Excepciones.**

  No obstante podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, y los que hagan referencia al origen racial, a la salud, y a la vida sexual, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, 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 sujeto al secreto profesional o por otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento (artículo 7.6 de la LOPD).

Esto es un ejemplo de lo que se consideran datos especialmente protegidos o sensibles.



6. La Agencia Española de Protección de Datos

El art. 35 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), establece que:

> *La Agencia Española de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones.*

El art. 1.2 del EAEPD dispone que la Agencia actúe con plena independencia de las administraciones públicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia.

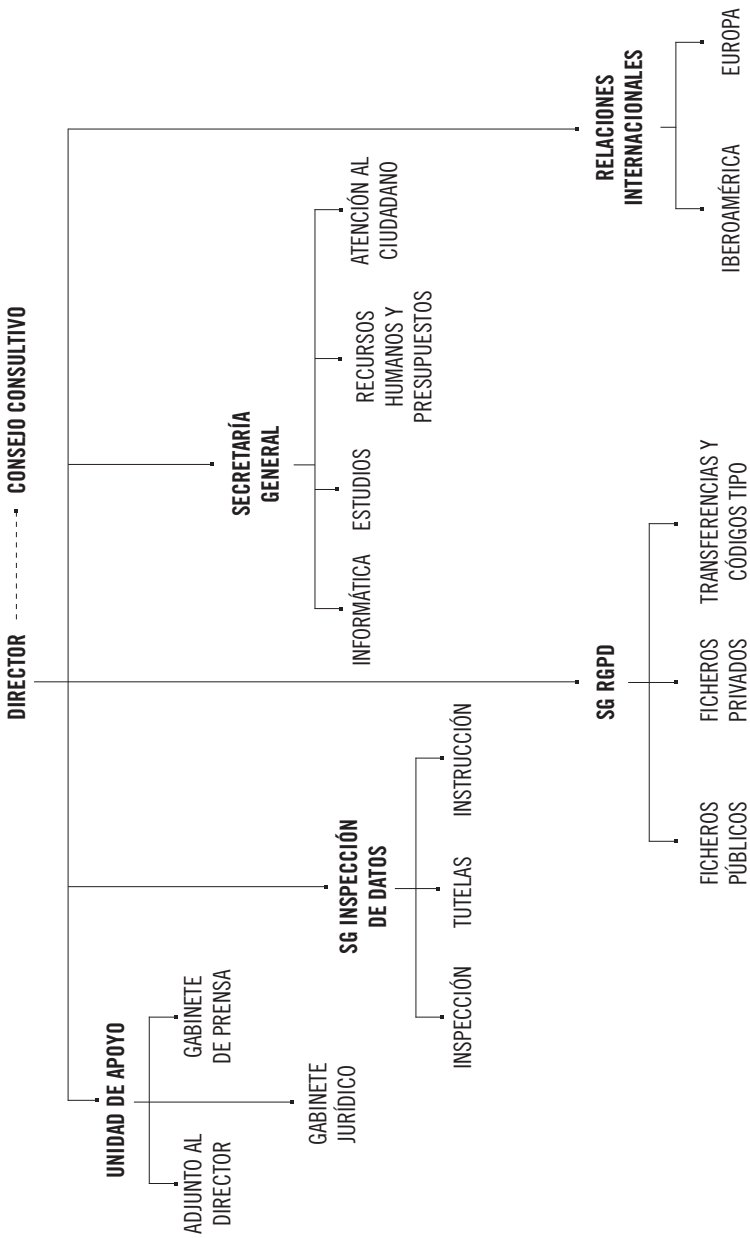
Recuerde

La Agencia Española de Protección de Datos (en lo sucesivo AEPD) es el ente de derecho público que vela por el cumplimiento de la normativa sobre protección de datos personales, actuando para ello con plena independencia de las Administraciones Públicas.

En este sentido:

- **INFORMA:** sobre el contenido, los principios y las garantías del derecho fundamental a la protección de datos regulado en la LOPD.
- **AYUDA:** al ciudadano a ejercitar sus derechos y a los responsables y encargados de tratamientos a cumplir las obligaciones que establece la LOPD.
- **TUTELA:** al ciudadano en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición cuando no han sido adecuadamente atendidos por los responsables de los ficheros.
- **GARANTIZA:** el derecho a la protección de datos investigando aquellas actuaciones de los responsables o encargados de ficheros que puedan ser contrarias a los principios y garantías contenidos en la LOPD. Impone, en su caso, la correspondiente sanción.

La estructura orgánica de la AEPD es la siguiente:


DIRECTOR
CONSEJO CONSULTIVO
UNIDAD DE APOYO
ADJUNTO AL DIRECTOR
GABINETE DE PRENSA
GABINETE JURÍDICO
SG INSPECCIÓN DE DATOS
INSPECCIÓN
TUTELAS
INSTRUCCIÓN
SECRETARÍA GENERAL
INFORMÁTICA
ESTUDIOS
RECURSOS HUMANOS Y PRESUPUESTOS
ATENCIÓN AL CIUDADANO
SG RGPD
FICHEROS PÚBLICOS
FICHEROS PRIVADOS
TRANSFERENCIAS Y CÓDIGOS TIPO
RELACIONES INTERNACIONALES
IBEROAMÉRICA
EUROPA

6.1. Funciones de la Agencia Española de Protección de datos

Las funciones que se le atribuyen a la AEPD, se enmarcan dentro del objeto de vigilancia del cumplimiento de la legislación sobre protección de datos, y controlar su aplicación, en especial en lo relativo a los derechos, de información, acceso, rectificación, oposición, y cancelación de datos.

Estas funciones se pueden desglosar de la siguiente forma:

- En relación a los afectados:

  a. Atender las peticiones y reclamaciones formuladas por las personas afectadas.
  b. Proporcionar información a las personas, acerca de sus derechos en materia de tratamiento de los datos de carácter personal.
  c. Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, y publicar periódicamente una relación de dichos ficheros, con la información adicional que el director de la agencia determine.

- En relación con quienes tratan datos:

  a. Emitir las autorizaciones previstas en la ley, o en sus disposiciones reglamentarias.
  b. Requerir a los responsables y los encargados de los tratamientos previa audiencia de estos, la adopción de medidas para la adecuación del tratamiento de los datos a las disposiciones de esta ley.
  c. Ordenar, en caso de ilegalidad, el cese en el tratamiento y cancelación de los datos.
  d. Ejercer la potestad sancionadora, en los términos previstos por el Título VII de la presente ley.
  e. Recabar a los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.
  f. Ejercer el control, y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, y desempeñar funciones de cooperación internacional en materia de protección de datos.

- En la elaboración de las normas:

  a. Informar con carácter preceptivo, los proyectos de disposiciones generales que desarrollan esta ley.
  b. Dictar las instrucciones precisas, para adecuar los tratamientos a los principios de la presente ley.
  c. Dictar las instrucciones precisas, sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos.
  d. Las resoluciones de la Agencia Española de la Protección de Datos se harán públicas, una vez hayan sido notificados a los interesados. La publicación se realizará a través de medios informáticos o telemáticos.

- En materia de telecomunicaciones:

  a. Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico, o medios de comunicación electrónica o equivalente.

- Otras funciones:

  a. Velar por la publicidad en los tratamientos, publicando anualmente una lista de los mismos.
  b. Cooperación internacional.
  c. Representación y observancia de lo dispuesto en la ley reguladora de la función Estadística Pública.
  d. Elaboración de una memoria anual, presentada por conducto del Ministro de Justicia a las Cortes Generales.

6.2. Otras funciones especifícas de la Agencia Española de Protección de Datos

A continuación se van a presentar otras funciones menos habituales de la Agencia Española de Protección de Datos.

La Inspección de Datos

- **Función**
  - Comprobación de la legalidad de los tratamientos.
  - Organización:
    - Inspectores de datos.
    - Instrucción de procedimientos.
    - Tutelas de derechos.
    - Procedimientos sancionadores.
    - Procedimientos de infracción por las Administraciones Públicas.
- **Funciones inspectoras**
  - Naturaleza de autoridad pública.
  - Deber de secreto de los inspectores.
  - Posibles actuaciones:
    - Examen de soportes.
    - Examen de equipos.
    - Análisis de programas.
    - Examen de los sistemas de transmisión.
    - Auditoria informática.
    - Requerimiento de información.
  - Potestades de entrada en locales.
  - Supuestos de actuación.
    - Ante una denuncia de un afectado o en supuestos de "alarma social".
    - Dentro de un plan de inspección de oficio.
    - Planes de Oficio Finalidad "preventiva".

Solo se imponen sanciones en casos de extrema gravedad
Tiene por objeto conocer el modo en que se realizan los tratamientos por parte de un sector.

Concluye con la preparación de unas "recomendaciones" en que se detectan los problemas.

- **Instrucción de procedimientos. Tutela de derechos.**
  - Presupuesto:
    - Ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición.
    - Denegación de este derecho por el responsable del Fichero.
  - Procedimiento:
    - Reclamación por escrito a la APD.
    - La APD requiere alegaciones al responsable en plazo de 15 días.
    - Práctica de pruebas o inspección.
    - Audiencia del responsable y el afectado.
    - Resolución.
    - Plazo máximo de tramitación: 6 meses. Silencio positivo.

- **Instrucción de procedimientos. Procedimiento sancionador.**
  - Causa de iniciación:
    - Denuncia de un afectado.
    - Conocimiento de un hecho presuntamente ilícito (por ejemplo, por los medios de comunicación o denuncia de un tercero).
  - Procedimiento:
    - Establecido por las normas generales de derecho administrativo (R. D. 1398/1993, de 4 de agosto, en desarrollo Título VI Ley 30/1992).

- **Medidas cautelares específicas.**

- En caso de hechos tipificados como infracción muy grave de utilización o cesión ilícita.
- Perjuicio para los derechos de los ciudadanos y el libre desarrollo de la personalidad.
- Podrá requerirse el cese en el tratamiento.
- Si no se atiende, podrán inmovilizarse los ficheros.

- **Instrucción de procedimientos.**

  - Procedimiento sancionador. Contenido de la resolución sancionadora.
  - Ficheros de titularidad privada:

    - Multa económica (criterios de cuantificación y atenuación previstos en la Ley).
    - Medidas complementarias.

  - Ficheros de titularidad pública:

    - Declaración de la infracción.
    - Imposición de medidas correctoras.
    - Solicitud de medidas disciplinarias para el responsable de la actuación ilícita.
    - Notificación de la resolución al Defensor del Pueblo.

Recuerde

Recuerde que para cualquier consulta se puede dirigir a:

- Al teléfono 901 100 099.
- Al fax 91 445 56 99
- A través de correo electrónico ciudadano@agpd.es.
- Visitando la página Web: www.agpd.es.
- Por correo a la: Agencia Española de Protección de Datos, Jorge Juan 6 - 28001 Madrid.

Ejercicios de repaso y autoevaluación

1. ¿Cuál es la finalidad de la protección de datos?

_____
_____
_____
_____

2. Para la recogida de datos de origen racial es necesario el consentimiento del interesado...

a. ... de manera tácita.
b. ... por escrito.
c. ... de manera expresa y por escrito.
d. ... de manera expresa.

3. ¿Pueden obligarme a declarar sobre mi ideología, religión o creencias?

_____
_____
_____
_____

4. Los datos de salud relativos al el grado de incapacidad de una persona, ¿qué nivel de seguridad tienen?

a. Nivel básico.
b. Nivel alto.
c. Nivel medio.

5. ¿Qué nivel de seguridad tienen los datos relativos a servicios financieros?

a. Alto.
b. Medio.
c. Básico.

6. **¿Qué nivel de seguridad se le aplicaría a los ficheros que contienen datos bancarios, tarjetas de crédito, rentas...?**

    a. Alto.
    b. Medio.
    c. Básico.

7. **¿Pueden ser objeto de tratamiento los datos de carácter personal que revelen la ideología afiliación sindical, religión y creencias?**