LEY ORGÁNICA DE PROTECCION DE DATOS. CURSO 2017

PORTAFOLIO COECO

Hecho por: Juan Vicente Ramos García

2017

**TEMARIO**

1. **Introducción**
   1. Introducción
   2. Definiciones (Conceptos Básicos)
   3. ¿Cuál es el objetivo de la LOPD?
   4. ¿A quién afecta la LOPD? Ámbito de aplicación.
   5. Ficheros que no regula la LOPD
2. **DATOS DE CARÁCTER PERSONAL**
   1. Principio de calidad de datos
   2. Derecho de los interesados a la información durante la recogida de datos
   3. Consentimientos del afectado
      1. Como recabar el consentimiento
      2. Como revocar el consentimiento
   4. Tipos de Datos
   5. Datos especialmente protegidos
   6. El deber es Secreto
3. **MOVIMIENTO DE DATOS**
   1. Comunicación de los datos a terceros
   2. Acceso de los datos por cuenta de terceros
      1. La subcontratación
   3. Movimiento internacional de datos
4. **FICHEROS DE TITULARIDAD PRIVADA**
   1. Creación y notificación del fichero
   2. ¿Dónde puedo crear un fichero?
   3. ¿Debo notificar la creación o existencia de un fichero?
   4. Clasificación de ficheros
   5. ¿Qué tipo de cambios hay que notificar a la AEPD?
   6. Especificaciones sobre algún tipo de ficheros
      1. Los datos incluidos en las fuentes de acceso publico
      2. El Censo Promocional
      3. La prestación de servicios sobre solvencia patrimonial
      4. Los tratamientos con fines de publicidad y de prospección comercial
   7. Los códigos tipo
      1. Contenido mínimo de un código tipo
   8. La Auditoria
5. **EL DOCUMENTO DE SEGURIDAD**
   1. La seguridad de los datos
   2. El Documento de Seguridad
   3. Los niveles de seguridad en los datos
      1. Nivel Básico
      2. Nivel Medio
      3. Nivel Alto
   4. Contenido mínimo de los Documentos de Seguridad
      1. Documentos de Seguridad de Nivel Básico
      2. Documentos de Seguridad de Nivel Medio
      3. Contenido del Documentos de Seguridad de Nivel Alto
6. **Ficheros de Titularidad Publica**
   1. Ficheros de titularidad pública
7. **LOS DERECHOS DE LAS PERSONAS**
   1. Introducción
   2. Derecho a ser informado de la recogida y del tratamiento de los datos
   3. Derecho a que sea recabado su consentimiento
   4. Derecho de Acceso
   5. Derecho de Cancelación
   6. Derecho de Rectificación
   7. Derecho de Oposición
   8. Derecho de Indemnización
   9. Derecho de consulta en el Registro Gral. De Protección de Datos
   10. Derecho de impugnación de valoraciones
   11. Derecho de exclusión de las guías telefónicas
   12. Derecho a no recibir publicidad no deseada
   13. Derechos de abonados y usuarios de servicios de telecomunicaciones
8. **INFRACCIONES Y SANCIONES**
   1. Infracciones leves
   2. Infracciones graves
   3. Infracciones muy graves
9. **LA AGENCIA DE PROTECCION DE DATOS**
   1. La Agencia Española de Protección de Datos
   2. La página web de la Agencia De Protección de Datos
10. **RECAPITULACION**
    1. ¿Qué es la LOPD?
    2. ¿Por qué se debe de aplicar la LOPD?
    3. ¿Qué requisitos hay que llevar a cabo para cumplir la LOPD?

ANEXO

1. introduccion
   1. introduccion

Derecho a la intimidad de las personas no es nada nuevo. 1944, se reconocía en la Declaración Universal de los Derechos Humanos. La 1ª ley en Europa se redactó en Alemania en 1970. En EE. UU. en 1974 se dictó la *Privacy Act.*

En España se reconoce desde 1978 con el Art. 18 de la Constitución, el cual dice que cualquier persona tiene derecho a controlas todos los aspectos de su vida privada y decidir quién puede acceder a sus datos y quién no.

1992. Debido a la generalización de la informática en las empresas se redacta la Ley Orgánica 5/1992(LORTAD) para regularizar el tratamiento automatizado de datos de carácter personal. Se promulgo el decreto 994/1999 para dar cumplimiento al art.9 de la LORTAD.

En 1995 la UE aprueba la directiva95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en tratamiento de datos personales y libre circulación de datos con la función de proteger los derechos fundamentales (derecho a la intimidad).

1999 se dicta la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), cuyo ámbito de aplicación son los datos de carácter personal registrados en soporte físico, automatizados o no. Con la LOPD se pretende mejorar las carencias de la LORTAD. En 2007 se aprueba el Real Decreto 1720/2007 por el que se aprueba el Reglamento de la LOPD.

* 1. DEFINICIONES

Datos de Carácter Personal: Información numérica, alfabética, grafica, fotográfica, acústica o de cualquier tipo concerniente a personas físicas identificadas e identificables

Datos de carácter personal relacionados con la salud: informaciones concernientes a la salud pasada, presente y futura, física o mental de un individuo. Se consideran los referidos a su % de discapacidad y a su información genética.

Fichero: Todo conjunto organizado de datos de carácter personal que permita el acceso a datos con arreglo a criterios determinados, sea cual sea su forma o modalidad de creación, almacenamiento, organización y acceso

Fichero no automatizado: Todo conjunto de datos de carácter personal org. De forma no automatizada y estructurado según criterios específicos relativos a personas físicas que permitan acceder sin esfuerzo a sus datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.

Ficheros temporales: Ficheros de trabajo creados por usuario o procesos que son necesarios para un tratamiento ocasional o como pasos intermedios durante la realización de un tratamiento.

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

Responsable del fichero o tratamientos: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que solo o juntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

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.

Encargado del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que solo o juntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio

Afectado o Interesado: Persona física titular de los datos que sean objeto de tratamiento

Comunicación o cesión de datos: Tratamiento de datos que supone su revelación a una persona distinta del interesado.

Destinatario o Cesionario: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo al que se revelen los datos. Podrán también ser destinatarios, entes sin responsabilidad jurídica que actúen en el tráfico como sujetos diferenciados.

Transferencia de Datos: Transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo u otro medio convencional.

Fuentes accesibles al público: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona no impedida por una norma limitativa, o sin más exigencia que en su caso, una contraprestación.

Sistema de información: Conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal

Sistema de tratamiento: Modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información pueden ser automatizados, no automatizados o parcialmente automatizados.

Usuario: Sujeto o proceso autorizado para acceder a datos o recursos.

Recurso: Cualquier parte componente de un sistema de información.

Soporte: Objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado por un sistema de información y sobre el cual se puede grabar o recuperar datos.

Identificación: Procedimiento de reconocimiento de la identidad de un usuario.

Autenticación: Procedimiento de comprobación de la identidad de un usuario.

Control de Acceso: Mecanismo que, en función de la identificación ya autenticada, permite acceder a los fatos o recursos.

Contraseña: información confidencial (cadena de caracteres) que puede ser usada en la autenticación de un usuario o accedo a un recurso.

Copia de Respaldo: Copia de datos de un fichero automatizado en un soporte que permita su recuperación.

Incidencia: Anomalía que pudiese afectar a la seguridad de los datos.

Perfil de Usuario: Accesos autorizados a un grupo de usuarios

Documento: Todo escrito, grafico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada

Cancelación: Procedimiento mediante el responsable cesa en el uso de los datos. Esto impedirá el bloque de los datos consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Admón. Publicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y solo durante el plazo de prescripción de estas.

Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca especifica e informada, por la que el interesado consiente el tratamiento de datos personales.

Exportador de Datos Personales: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo situado en el territorio español que realice una transferencia de datos de carácter personal a un país tercero, conforme a lo dispuesto en el presente Reglamento.

Importador de Datos Personales: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea el responsable del tratamiento, encargada del tratamiento o tercero.

Persona Identificable: Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier info referida a su identidad física, fisiológica, psíquica, económica, cultural o social. No se considerará identificable si requiere plazos o actividades desproporcionados dicha identificación.

Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.

Tercero: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo autoridad directa del responsable del tratamiento o encargado del tratamiento. Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

* 1. ¿Cuál ES EL OBJETIVO DE LA LOPD?

Garantizas y proteger, en lo concerniente al tratamiento de datos personales, las libertades públicas y los dchos. Fundamentales de las personas físicas, y especialmente a su honor e intimidad personal y familiar.

* 1. ¿A QUIEN AFECTA LA LOPD? AMBITO DE APLICACIÓN

LOPD protege los datos de carácter personal registrados en soporte físico que sean susceptibles de tratamiento. Se aplica tanto a datos registrados en soporte automatizado como en soporte papel.

Esta ley se aplica a los sectores público y privado.

Se aplicará a:

-Personas físicas o jurídicas dentro del territorio español que realicen actividades en un establecimiento del responsable del fichero

-Las personas físicas y jurídicas a las cuales, aunque no se encuentren en territorio español, se les pueda aplicar la legislación española en aplicación de las normas de Dcho. Internacional Publico.

-Los responsables del tratamiento que, aunque no se encuentren en la UE, utilicen el tratamiento de datos medios que estén situados en Territorio Español a menos que se utilicen con fines de tránsito.

No se aplicará a:

-Ficheros que posean personas físicas para fines exclusivamente personales o domésticos que forman parte de la vida privada o familiar de los particulares.

-Ficheros sometidos a la normativa sobre protección de materias clasificadas

-Ficheros establecidos para la investigación del terrorismo y otras formas graves de delincuencia organizada

No obstante, en estos supuestos el responsable del fichero comunicara previamente la existencia del fichero, sus características generales y su finalidad a la AEPD.

También estarán excluidos del ámbito de aplicación de la protección de datos de carácter personal los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciales, industriales o navieros.

Tampoco se aplicará este Reglamento a personas fallecidas. No obstante, los familiares o las personas vinculadas al fallecido por razones análogas podrán dirigirse a los responsables de los ficheros que contengan datos de este con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo y solicitado, si se da el caso, la cancelación de los datos.

* 1. FICHEROS QUE NO REGULA LA LOPD

-Ficheros regulados por la legislación de régimen electoral

-Ficheros que sirven para fines exclusivamente estadísticos y estén amparados por la legislación estatal o autonómica sobre la función estadística publica

-Ficheros 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.

-Ficheros derivados del Registro Civil y del Registro Central de penados y rebeldes.

-Ficheros procedentes de imágenes y sonidos obtenidos mediante utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, conforme a la legislación sobre la materia.

1. LOS DATOS DE CARÁCTER PERSONAL

2.1 PRINCIPIO DE CALIDAD DE LOS DATOS

Art. 3 de la LOPD define dato de carácter personal “Cualquier info concerniente a personas físicas identificadas e identificables”. En gral. Se entiende por dato personal cualquier info sobre una persona determinada que permita conocer sus características personales.

Para cumplir el ppio. de Calidad el art 3 de la LOPD y el art. 8 el Reglamento dicen que los datos de carácter personal solo se podrán recoger y someter a tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explicitas y legitimas para las que se hayan obtenido.

No se podrán usar los datos de carácter personal para fines incompatibles con aquellos para los que se hubieran recogido, salvo fines históricos, estadísticos y científicos. (que no se considera una finalidad incompatible)

Además, está prohibida la venta fraudulenta, desleal o ilícita de datos de carácter personal. (siendo una infracción muy grave (300.505,05€ - 601.012,10€)

Los datos de carácter personal deben cumplir estos requisitos:

-Deben ser exactos y estar actualizados de forma que respondan verazmente a la situación actual del afectado. Cuando los datos se recojan directamente del afectado se consideran exactos.

-Si los datos de carácter personal sometidos a tratamiento fuesen inexactos, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en diez días desde el conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o plazo específico para ello.

-En el caso de que los datos que se deban rectificar o modificar hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar el cesionario, en 10 días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido. El cesionario deberá proceder a la rectificación y cancelación notificada, en diez días desde la recepción de la notificación. Esta actualización de los datos no requerirá comunicación alguna al interesado, aunque si podrá ejercer sus derechos en la LOPD.

-Cuando los datos sean total o parcialmente inexactos serán cancelados y sustituidos de oficio por los datos rectificados o completados.

-Los datos personales serán cancelados cuando dejen de ser necesarios o pertinentes para la finalidad para la que fueron recogidos. Además, tampoco se podrán conservar de forma que se pueda identificar a la persona interesada por un tiempo superior al necesario para cumplir la finalidad para la que fueron recabados.

-Podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado. Una vez cumplido el periodo, los datos solo podrán ser conservados siempre que hayan sido previamente disociados sin perjuicio de la obligación de bloque prevista en el LOPD y Reglamento.

-Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

-Los datos personales se almacenarán de forma que se permita el ejercicio del derecho de acceso (excepto cuando hayan sido legalmente cancelado).

2.2 EL DCHO DE LOS INTERESADOS A LA INFORMACION DURANTE LA RECOGIDA DE DATOS

Todos los interesados a los que se le soliciten datos personales deberán estar previamente informados de forma precisa, inequívoca y expresa de:

-La existencia de un fichero o tratamiento de datos de carácter personal

-La finalidad de la recogida de estos datos.

-Los destinatarios de esta información

-El carácter obligatorio o facultativo de su respuesta a las preguntas planteadas

-Las consecuencias de la obtención de los datos o la negativa a suministrarlos. La posibilidad de ejercitar los derechos de acceso rectificación, cancelación y oposición.

-Por último, la identidad y dirección del responsable del tratamiento, o, en su caso, de su representante.

El deber de información debe llevarse a cabo a través de un medio que permita acreditar su cumplimiento. El responsable del fichero deberá conservar el soporte en el que conste el cumplimiento del deber de informar durante el periodo de tiempo el cual transcurra el tratamiento de datos.

Cuando los datos no se recaben directamente de la persona interesada, el responsable del fichero o su representante deberá informar a esa persona de manera expresa, precisa e inequívoca antes de los tres meses siguientes al momento del registro de los fatos, a menos que:

-La obtención de dicha info haya sido prevista por alguna ley

-El tratamiento tenga fines históricos, estadísticos o científicos

-La información al interesado sea imposible o exija esfuerzos desproporcionados a criterios de la APD o del organismo autonómico equivalente.

- Los datos procedan de fuentes accesibles al público y se destinen a actividades de publicidad o prospección comercial.

-En este último caso, en cada comunicación que se dirija al interesado, deberá informársele del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

2.3 EL CONSENTIMIENTO DEL AFECTADO

Salvo que la Ley disponga lo contrario, para poder tratar datos de carácter personal será siempre necesario el consentimiento inequívoco del afectado, pudiendo revocarlo siempre que exista una causa justificada para ello, aunque no tendrá efectos retroactivos.

No será necesario el consentimiento:

-Cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Admón. Publicas en el ámbito de sus competencias.

-Cuando se refieran a las partes de un contrato o precontrato de una relación de negocios, laboral o administrativa y los datos sean necesarios para su mantenimiento y cumplimiento.

-Cuando la finalidad de los datos personales sea proteger un interés vital del interesado, como diagnósticos y tratamientos médicos.

-Cuando los datos se encuentren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero.

-Lo autorice una norma con rango de ley o una norma de dcho. Comunitario.

Aunque no sea necesario el consentimiento en los casos anterior, podrá oponerse a su tratamiento siempre que existan motivos fundados y legítimos relativos a una concreta situación personal y que no exista ley que disponga lo contrario. En este caso, el responsable del fichero deberá excluir del tratamiento los datos relativos al afectado.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, debiendo especificar la finalidad para la que se recaban los datos, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

Cuando se solicite el consentimiento del afectado para la cesión de sus datos deberá informarse a este de forma que conozca inequívocamente la finalidad a la que se destinaran los datos respecto de cuya comunicación se solicita el consentimiento y tipo de actividad desarrollada por el cesionario. En caso contrario el consentimiento será nulo.

El Reglamento trata en el art 13 la forma de recabar el consentimiento para el tratamiento de datos de menores de edad: “Podrá procederse al tratamiento de los datos de los mayores de 14 años con su consentimiento, salvo en aquellos casos en los que la Ley exija la para su prestación la asistencia de los titulares de la patria potestad o tutela. EN el caso de <14 años, se requerirá el consentimiento de padres o tutores”. Además, la info que se dirija a los menores deberá estar expresada de forma clara y comprensible.

En ningún caso podrán recabarse a través del menor datos que permitan obtener información sobre los demás miembros del grupo familiar o sobre las características del mismo, como actividad profesional de los progenitores, info económica, datos sociológicos o cualquiera sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización de los mismos.

Le corresponde al responsable del fichero articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso por los padres, tutores o representantes legales.

2.3.1 COMO RECABAR EL CONSENTIMIENTO

El responsable podrá dirigirse al afectado, informándole de

-La existencia de un fichero o tratamiento de datos de carácter personal

-La finalidad de la recogida de los datos

-Los destinatarios de esta información

-El carácter obligatorio o facultativo de su respuesta a las preguntas planteadas

-Las consecuencias de la obtención de los datos o la negativa a suministrarlos. La posibilidad de ejecutar los dchos de acceso, rectificación, cancelación y oposición

-Por último, la identidad y dirección del responsable del tratamiento, o, en su caso, de su representante.

Tras dicha comunicación deberá conceder al afectado un plazo de 30 días para manifestar su negativa, advirtiéndole de que en caso de no pronunciarse se entenderá que consiente el tratamiento de sus datos de carácter personal.

Cuando el responsable del fichero este prestando al afectado un servicio que genere info periódica o reiterada, o facturación periódica, la comunicación podrá llevare a cabo de forma conjunta a esta info o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

En cualquier caso, es necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido devuelta por algún motivo. En este caso, no se podrán tratar los datos referidos a ese afectado.

Los interesados podrán oponerse al tratamiento de sus datos a través de un medio sencillo y gratuito. Serian validos los procedimientos en el que tal negativa pueda efectuarse, por ejemplo, mediante un envío prefranqueado al responsable de tratamiento, una llamada a un nº gratuito o a un servicio de atención al público.

Cuando la finalidad para la cual se solicite el consentimiento del afectado no esté directamente relacionada con el servicio que se le está prestando, se debe permitir al mismo la posibilidad de manifestar su negativa al tratamiento o comunicación de datos. Por ejemplo, la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento contractual que se le entregue sería un medio correcto para cumplir con esta obligación.

2.3.2 COMO REVOCAR EL CONSENTIMIENTO

Los afectado podrán revocar el consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. Sera valido cualquier procedimiento en el que la revocación pueda efectuarse, p.e mediante un envío prefranqueado al responsable de tratamiento, una llamada a un nº gratuito o a un servicio de atención al público.

No se consideran válidos, los casos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualquier medio que impliquen un coste adicional.

El responsable deberá cesar el tratamiento de los datos en el plazo máximo de 10 días a contar desde el de la recepción de la revocación del consentimiento. Si el interesado hubiera solicitado del responsable la confirmación del cese, este deberá responder expresamente a la solicitud.

Si los datos, hubieran sido cedidos o comunicados previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlos a los cesionarios, en el plazo de 10 días, para que estos, cesen el tratamiento de los datos en caso de que aún lo mantuvieran.

2.4. TIPOS DE DATOS

DATOS ESPECIALMENTE PROTEGIDOS:

* Ideología
* Afiliación sindical
* Religión
* Creencias
* Origen Racial o Étnico
* Salud
* Vida Sexual

DATOS DE CARÁCTER IDENTIFICATIVO

* DNI/NIF
* N.º S.S/Mutualidad
* Nombre y Apellidos
* Dirección (Postal electrónica)
* Teléfono
* Firma/Huella digital
* Imagen/Voz
* Marcas Físicas
* Firma Electrónica

DATOS DE CARACTERISITICAS PERSONALES

* Datos de estado civil
* Datos de familia
* Fecha de nacimiento
* 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 ACADEMICOS Y PROFESIONALES

* Formación, titulaciones
* Historial de estudiante
* Experiencia profesional
* Pertenencia a colegios o asociaciones profesionales

DATOS DE DETALLES DE EMPLEO

* Profesión
* Puesto de trabajo
* Datos no económicos de nomina
* Historial del trabajador

DATOS DE INFORMACION COMERCIAL

* Actividades y negocios
* Licencias comerciales
* Suscripciones a publicaciones/medios de comunicación
* Creaciones artísticas, literarias, científico-técnicas

DATOS ECONOMICOS, FINANCIEROS Y DE SEGUROS

* Ingresos, rentas
* Inversiones, bienes patrimoniales
* Créditos, prestamos avales
* Datos bancarios
* Planes de pensiones, jubilación
* Datos económicos de nomina
* Datos deducciones impositivas/impuestos
* Seguros
* Hipotecas
* Subsidios, beneficios
* Historial créditos
* Tarjetas crédito

DATOS DE TRANSACCIONES

* Bienes y servicios suministrados por el afectado
* Bienes y servicios recibidos por el afectado
* Transacciones financieras
* Compensaciones, indemnizaciones

2.5. DATOS ESPECIALMENTE PROTEGIDOS

-Ideología

-La afiliación sindical

-La religión

-Las creencias

Estos datos únicamente podrán ser objeto de tratamiento con el consentimiento expreso y por escrito del afectado. Además, debe informarse de forma expresa al afectado que tiene derecho a no prestar dicho consentimiento de acuerdo con el art 16 apartado 2 de la constitución el que se establece que nadie podrá ser obligado a declarar sobre esos datos.

Los ficheros mantenidos por partidos políticos, sindicatos, iglesias, comunidades religiosas, asociaciones, fundaciones o entidades sin ánimo de lucro quedan excluidos, ya que estos ficheros tratarían datos de sus miembros o asociados. Por supuesto la cesión de estos datos precisara siempre el consentimiento previo del afectado.

Los datos sobre datos especialmente protegido podrán ser tratados únicamente en el caso de que sea necesario para la prevención diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios. También podrán ser tratados los datos citados anteriormente en el caso de que dicho tratamiento sea necesario para salvaguardar el interés vital de la persona afecta o de otra persona, en el supuesto de que el afectado este físico o jurídicamente incapacitado para dar su consentimiento.

Los ficheros creados con la única finalidad de almacenar datos personales sobre la ideología, la afiliación sindical, la religión, las creencias, el origen racial o étnico, o la vida sexual están totalmente prohibidos.

Los datos relacionados con la comisión de infracciones penales o administrativas solo podrán ser incluidos en los ficheros de las Admón. Públicas competentes, siempre en los supuestos previstos en las respectivas normas reguladoras.

Los datos personales relativos a la salud están también especialmente protegidos. Por eso para su tratamiento, será necesario el consentimiento expreso del afectado, o que el tratamiento se realice por razones de interés general o que así lo disponga una Ley.

Este consentimiento no será necesario en los casos de instituciones y centros sanitarios públicos y privados y los profesionales correspondientes que podrán proceder al tratamiento de los datos relativos a la salud de las personas que acudan a estos centros o que deban ser tratadas en los mismos.

Aunque la LOPD no hace una definición concreta de datos de salud, en el apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa se define este término como “las informaciones concernientes a la salud pasada, presente y futura, física o mental de un individuo” pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido. En los datos referentes a la salud se incluyen igualmente las info relativas al abuso de alcohol y consumo de drogas.

2.6. EL DEBER DE SECRETO

El responsable del fichero y todas las personas 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

El deber de secreto subsiste aun después de finalizar sus relaciones con el titular del fichero o en su caso con el responsable del mismo

3.MOVIMIENTO DE DATOS

3.1 COMUNICACIÓN DE LOS DATOS A TERCEROS

Solo se podrán comunicar datos de carácter personal a un tercero cuando dicha comunicación se realice para cumplir “fines directamente relacionados con las funciones legitimas del cedente y cesionario con el previo consentimiento del interesado”. Según el art 27 de la LOPD el responsable del fichero, en el momento de la primera cesión de datos, deberá informar de ello a los afectado.

Además, para que el consentimiento del interesado sea válido la info que se facilite debe permitirle conocer

-La finalidad a la que se destinaran los datos personales cuya comunicación está autorizando

-La naturaleza de los datos cedidos

-Nombre y dirección del cesionario.

El responsable del fichero no estará obligado a informar al afectado:

-Cuando la cesión la autorice una ley

-Cundo el tratamiento responda a la libre y legitima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros

-Cuando la comunicación que deba efectuarse se tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de sus funciones. Tampoco será necesario el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

-Cuando la comunicación se realice entre Admón. Publicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

-En el caso de que el tratamiento de los datos personales se realice mediante un procedimiento de disociación.

El consentimiento para l comunicación de los datos de carácter personal tiene carácter revocable.

Obviamente aquel a quien se comuniquen los datos está obligado al cumplimiento de la LOPD.

Existen situaciones en las que no es preciso el consentimiento del afectado para comunicación de datos personales:

* Cuando la cesión está autorizada en una ley
* Cuando los datos hayan sido recogidos de fuente accesibles al público
* Cuando el tratamiento responsa a la libre y legitima aceptación de una relación jurídica cuyo desarrollo cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros
* Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, al Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas en el ejercicio de sus funciones. Tampoco será necesario el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicos con funciones análogas al Defensor del Pueblo o el Tribunal de Cuentas
* Cuando la comunicación se realice entre Admón. Publicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos,
* Cuando la cesión de los datos relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Es importante señalar que en el caso de los ficheros de datos personales recabados de fuentes accesibles al público no es preciso solicitar el consentimiento al interesado, pero sí de la existencia del fichero

3.2 EL ACCESO A LOS DATOS POR CUENTA DE TERCEROS

Cuando un tercero necesita para poder prestar un servicio al responsable del tratamiento, acceder a los datos de carácter personal, deberá regularse este tratamiento de datos en un contrato por escrito o de alguna forma que permita acreditar su celebración y contenido.

En dicho contrato se deben establecer expresamente:

* El encargado del tratamiento únicamente tratara los datos conforme a las instrucciones del responsable del tratamiento.
* No aplicara o utilizara los datos con fin distinto al que figure en dicho contrato ni los comunicara, ni siquiera para su conservación, a otras personas.
* Se deberán estipular las medidas de seguridad a que se refiere el art 9 de la LOPD referente a la seguridad de los datos que el encargado de los datos está obligado a implementar

Una vez finalizado el contrato, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato personal objeto del tratamiento.

En el caso de que el encargado del tratamiento diera otra finalidad a los datos, los comunicara o los utilizara de forma que incumpliera las estipulaciones del contrato, sería considerado, también, responsable del tratamiento y por lo tanto respondería personalmente de las infracciones que hubiera cometido. No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable comunique datos a un tercero designado por aquel, al que hubiera encomendado la prestación de un servicio.

El responsable del fichero deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de todo lo dispuesto en la LOPD y en el Reglamento.

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser devueltos o destruidos, al responsable del tratamiento o al encargado que este hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

El encargado del tratamiento conservara, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

Las obligaciones del encargado del tratamiento deben estar regulada en el Documento de Seguridad según los art. 82,83, 84, 85 y 86.

3.2.1 LA SUBCONTRATACION

No obstante, será posible la subcontratación sin necesidad de autorización siempre:7

-Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que vaya a subcontratar. Cuando no se identificase en el contrato la empresa, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación. 7

-Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

-Que el encargado del tratamiento y la empresa subcontratista formalicen un contrato, en cuyo caso, el subcontratista sería considerado encargado del tratamiento.

3.3 MOVIMIENTO INTERNACIONAL DE DATOS

En el art 33 de la LOPD se dice claramente que no se podrán transferir, temporal o definitivamente, datos de carácter persona que hayan sido objeto de tratamiento o que hayan sido recogidos para someterlos a dicho tratamiento a países que no garanticen un nivel de protección equiparable al que presta la LOPD. Esto quiere decir que, para transferir datos personales a un país extranjero, este debe cumplir primeramente todos los niveles de protección que se requieren en la LOPD, a menos que, además de observar todo lo que se dispone en esta, lo autorice previamente el director de la Agencia de Protección de Datos.

La APD es la encargada de evaluar el carácter adecuado de los niveles de protección de cada país.

Para decidir qué países lo cumplen se evaluarán los siguientes aspectos,

-La naturaleza de los datos de finalidad

-La duración del tratamiento o los tratamientos privados

-El país de origen

-El país de destino

-Las normas de Dcho. Generales o sectoriales vigentes en el país tercero

-El contenido de los informes de la Comisión dela UE

-Las normas profesionales y las medidas de seguridad en vigor en dichos países.

Existen caso en los que no es aplicable lo anterior

- Cuando la transferencia de los datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

-Cuando la transferencia se haga con la finalidad de prestar o solicitar auxilio judicial internacional

-Cuando la transferencia sea necesaria para la prevención o el diagnostico médicos, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios

-Cuando se trate de transferencias dinerarias conforme a su legislación especifica

-Cuando el afectado haya dado su consentimiento inequívoco a la transferencia

-Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afecto y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado

-Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

-Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Este será el caso de una Admón. Fiscal o aduanera que solicite la transferencia para cumplir sus competencias.

-Cuando la trasferencia será precisa para reconocimiento, ejercicio o defensa de un derecho en un proceso judicial

-Cuando la transferencia se efectúa a petición de una persona con interés legítimo desde un Registro público, y aquella sea acorde con la finalidad del mismo.

- Cuando la transferencia tenga como destino un estado miembro de la UE, os un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado

4.FICHEROS DE TITULARIDAD PRIVADA

4.1 CREACION Y NOTIFICACION DEL FICHERO

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

Según el art 55 del Reglamento, los ficheros de datos de carácter personal deberán notificarse a la AEPD por la persona o entidad privada que pretenda crearlos, previamente a su creación.

4.2 ¿CUÁNDO PUEDO CREAR UN FICHERO?

Según el art 25 de la LOPD, solo podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad de la empresa, persona, o entidad titular y se respeten las garantías que la LOPD establece para la protección de las personas.

4.3¿DEBO NOTIFICAR LA CREACION O EXISTENCIA DE UN FICHERO ¿

La creación de un fichero de datos de carácter personal debe notificarse previamente a la AEPD.

La notificación debe contener:

* Responsable del fichero
* Finalidad del fichero
* Ubicación del fichero
* Tipo de datos que contiene
* Medidas de seguridad (indicando el nivel de protección básico, medio o alto)
* Cesiones de datos que se prevean hacer
* Transferencias de datos que se prevean a países terceros.

La notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento de los datos. De igual modo, cuando los datos de carácter personal objeto de un tratamiento están almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado solo será precisa una sola notificación, referida a dicho fichero.

Cuando se tenga previsto crear un fichero del que resulten responsables varias personas o entidades simultáneamente, cada una de ellas deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos.

El Registro General de Protección de Datos inscribirá el fichero si la notificación reúne los requisitos que se exigen. En caso de que falte algún requisito el Registro es el encargado de pedir que se completen los datos que falten o que se subsanen los posibles errores.

El fichero automatizado quedara inscrito transcurrido un mes desde la presentación de la solicitud de inscripción, sí que la AEPD hubiera resuelto sobre la misma

La inscripción del fichero deberá encontrarse actualizada en todo momento.

4.3.1 FICHEROS PREEXISTENTES

Todos los ficheros automatizados preexistentes deberían haberse notificado a la AEPD antes del 14 de enero de 2003. Los ficheros no automatizados deberían haberse notificado a la Agencia antes del 24 de octubre de 2007.

4.4 CLASIFICACION DE FICHEROS

GESTION CONTABLE, FISCAL Y ADMINISTRATIVA

* Gestión económica y contable
* Gestión fiscal
* Gestión administrativa
* Gestión de facturación
* Gestión de clientes
* Gestión de proveedores
* Gestión de cobros y pagos
* Administración de fincas
* Consultorías, auditorias, asesorías y servicios relacionados
* Históricos de relaciones comerciales

RECURSOS HUMANOS

* Gestión de personal
* Gestión de nominas
* Formación de personal
* Prestaciones sociales
* Selección de personal
* Gestión de trabajo temporal
* Promoción y gestión de empleo
* Prevención riesgos laborales
* Control horario

SERVICIOS ECONOMICOS-FINANCIEROS Y SEGUROS

* Cuenta de crédito
* Cuenta de deposito
* Gestión de patrimonios
* Gestión de fondos de pensiones y similares
* Gestión de tarjetas de crédito y similares
* Registro de acciones y obligaciones
* Otros servicios financieros
* Cumplimiento/incumplimientos de obligaciones dinerarias
* Prestación de servicios de solvencia patrimonial y crédito
* Seguros de vida y salud
* Otro tipo de seguros

PUBLICIDAD Y PROSPECCIONS

* Publicidad
* Venta a distancia
* Encuestas de opinión
* Análisis de perfiles
* Prospección comercial
* Segmentación de mercados
* Sistemas de ayuda a la toma de decisiones
* Recopilación de direcciones

SERVICIOS DE TELECOMUNICACIONES

* Prestación de servicios de telecomunicaciones
* Guías/repertorios de servicios de telecomunicaciones
* Comercio electrónico
* Prestación de servicios de certificación

ACTIVIDADES ASOCIATIVAS, CULTURALES, RECREATIVAS, DEPORTIVAS Y SOCIALES

* Gestión de actividades culturales
* Gestión de clubes o asociaciones deportivas, culturales, profesionales y similares
* Gestión de asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro
* Actividades asociativas diversas
* Asistencia social
* Gestión de medios de comunicación social

EDUCACION

* Enseñanza infantil primaria
* Enseñanza secundaria
* Enseñanza universitaria
* Educación especial
* Otras enseñanzas

SANIDAD

* Gestión y control sanitario
* Historial clínico
* Investigación epidemiológica y actividades analógicas

SEGURIDAD

* Investigaciones privadas a personas
* Seguridad y control acceso a edificios
* Otras actividades de seguridad

FINALIDADES VARIAS

* Fidelización de clientes
* Reservas y emisión de billetes
* Fines históricos, científicos o estadísticos
* Otras finalidades

4.5 ¿Qué TIPOS DE CAMBIOS HAY QUE NOTIFICAR A LA AEPD?

Deberán notificarse:

-La finalidad del fichero automatizado

-El responsable

-La dirección de su ubicación

También deberá comunicarse a la AEPD cualquier modificación posterior en el contenido de la inscripción del fichero en el Registro Gral. De Protección de Datos

Cuando se decida suprimir un fichero el responsable del tratamiento o fichero deberá notificarlo a efectos de que se proceda la cancelación de la inscripción en el registro correspondiente.

4.6 ESPECIFICACIONES SOBRE ALGUNOS TIPOS DE FICHEROS

4.6.1 LOS DATOS INCLUIDOS EN LAS FUENTES DE ACCESO PUBLICO

La LOPD, en el art 3 considera fuentes de acceso público:

-El censo Promocional

-Listas de personas pertenecientes a grupos de profesionales que contengan únicamente nombre, titulo, profesión, actividad, grupo académico, dirección profesional e indicación de su pertenencia al grupo.

- Las guías de servicios de comunicaciones electrónicas

-Diarios y boletines oficiales

-Medios de comunicación social

Cualquier persona puede realizar consultas en estas fuentes, sin más exigencia, en algunos casos que el abono de una contraprestación.

Las fuentes de acceso público deben incluir los datos personales estrictamente necesarios para cumplir la finalidad para la que fueron destinados. En caso de incluir datos adicionales, las entidades responsables del mantenimiento de estas fuentes deberán solicitar el consentimiento del interesado, que podrá ser revocado en cualquier momento.

Los libros del registro y los archivos judiciales no se consideran fuentes accesibles al público, ya que no se encuentran a disposición del público en general, si no que el acceso a los mismos está regulado y, en cierta medida, restringido y sujeto a un trámite de solicitud y autorización.

En el caso de los Colegios Profesionales, los interesados tienen derecho a que la entidad responsable del mantenimiento de los listados de estos colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial.

La atención a la solicitud de objeción al uso de los datos con fines publicitarios deberá realizarse en el plazo de 10 días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en el que se edite.

Las fuentes de acceso público que se editen en forma de soporte físico perderán el carácter de fuente accesible con la nueva edición que se publique. Para el caso de las copias en formato electrónico, estas perderán el carácter de fuentes de acceso público en el plazo de un año, contado el momento de su obtención.

Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa especifica

4.6.1.1 ¿ES INTERNET UNA FUENTE DE ACCESO PUBLICO?

La AEPD considera que no lo es. Por lo tanto, es necesario obtener el consentimiento inequívoco, especifico e informado del afectado para realizar tratamiento con sus datos personales publicados en Internet, aunque estos se hayan publicado de forma que cualquier usuario de internet pueda acceder a los mismos.

4.6.2 EL CENSO PROMOCIONAL

Las empresas cuya actividad, permanente o esporádica, sea la recopilación de direcciones, el reparto de documentos, la publicidad, la venta a distancia, la prospección comercial u otras actividades análogas pueden solicitar una copia del censo promocional al Instituto Nacional de Estadística (u órgano equivalente de la C.A). El Censo Promocional contiene:

-Nombre y apellidos

-Domicilio que conste en el censo electoral

Puede utilizarse el censo promocional durante el plazo de un año. Transcurrido este plazo la lista perderá el carácter de fuente de acceso público.

Los interesados pueden solicitar no aparecer en dichos listados, es decir, tienen derecho a exigir que las entidades encargadas del mantenimiento de dichas fuentes la exclusión de todos sus datos personales gratuitamente. Estas deberían atender la solicitud en el plazo de 10 días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en el que se edite.

Se puede solicitar una contraprestación por la facilitación de la lista del censo promocional en soporte informático.

4.6.3 LA PRESTACION DE SERVICIOS SOBRE SOLVENCIA PATRIMONIAL Y CREDITO

Las personas o empresas que se dediquen a la prestación de servicios de información sobre solvencia patrimonial y crédito solo podrán tratar de datos de carácter personal que hayan obtenido de las fuentes accesibles al público o de informaciones facilitadas por el interesado o con su conocimiento.

También se podrán tratar los datos de carácter personal relativos al cumplimiento o no de obligaciones dinerarias cuando hayan sido facilitadas por el acreedor o por quien actué por su cuente o interés. Estos datos deberán conservarse en ficheros creados con la exclusiva finalidad de facilitar información crediticia del afectado.

Los datos de carácter personal deberán responder con veracidad a la situación de la deuda en cada momento concreto. El pago o cumplimiento de la deuda terminara la cancelación inmediata de todo dato relativo a la misma.

El tratamiento de este tipo de datos debe notificarse a los interesados en el momento en que se registren sus datos de carácter personal y en el plazo de treinta días desde este registro, realizando en dicha notificación una referencia de los datos que se han incluido en el fichero e informándoles de sus derechos, en los términos establecidos en la LOPD. Se efectuará una notificación por cada deuda concreta y determinada con independencia de que se esta se tenga con el mismo o con distintos acreedores. La notificación al afectado deberá efectuarse a través de un medio fiable, auditable e independiente de la entidad notificante, que le permita acreditar la efectiva realización de los envíos.

En todo caso, será necesario que el responsable del fichero pueda conocer si la notificación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado. Las devoluciones en las que el destinatario haya rehusado recibir el envió no se entenderán suficientes para que no se pueda proceder al tratamiento de los datos referidos a un interesado.

Cuando el interesado lo solicite, el responsable del tratamiento deberá comunicar los datos y, las evaluaciones y apreciaciones que se hayan comunicado sobre el interesado durante los últimos seis meses, y el nombre y la dirección de la persona o la entidad a quien se hayan revelado los datos.

Además, según el art 38 del reglamento, solo se podrán incluir en estos ficheros los datos de carácter personal que sean determinantes para poder enjuiciar la solvencia económica de los interesados, siempre que se den estos requisitos:

1.- Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previsto en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por el Real Decreto 303/2004 del 20 de febrero.

2.- Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquella fuera de vencimiento periódico.

3.- Requerimiento previo de pago a quien corresponsal el cumplimiento de la obligación

El acreedor deberá informar al deudor de la inclusión de los datos relativos, al impago en un fichero relativo al cumplimiento o incumplimiento de obligaciones dinerarias en el momento en que se celebre el contrato o, en el momento en que se envié el requerimiento previo de pago.

El acreedor o quien actué por su cuenta o interés deberá conservar a disposición del responsable del fichero común y de la AEPD documentación suficiente que acredité el cumplimiento de los requisitos establecidos en el art 38 del Reglamento y del requerimiento previo al que se refiere el art 39.

El ejercicio de los derechos por parte de los afectado podrá realizarse dirigiéndose al responsable del tratamiento o fichero o, a la persona o entidad a la que se presta el servicio. En este último caso, estas deberán comunicar al afectado los datos relativos al mismo que le hayan sido comunicados y facilitar la identidad del responsable para que, en su caso puedan ejercitar sus derechos ante el mismo.

Por último, cualquier tercero que precise enjuiciar la solvencia económica del afectado podrá acceder a la información contenida en el fichero siempre que se den los siguientes supuestos:

-Que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida

-Que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio

-Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica

4.6.4 LOS TRATAMIENTOS CON FINES DE PUBLICIDAD Y DE PROSPECCION COMERCIAL

Las personas o entidades que se dediquen a la recopilación de direcciones, el reparto de documentos, publicidad, venta a distancia, prospección comercial, y otras actividades análogas, así como las entidades que realicen estas actividades con el fin de comercializar sus propios productos o los de terceros solo podrán utilizar datos personales cuando hayan sido obtenidos de fuentes accesibles al público o cuando hayan sido facilitados por el propio interesado o con su consentimiento.

En cada comunicación que se dirija al interesado se le debe informar del origen de los datos, y de la identidad del responsable del tratamiento, así como los derechos que le asisten, entre ellos, el derecho de acceso y a oponerse al tratamiento de datos que le conciernen.

Para que una entidad pueda realizar por sí misma una actividad publicitaria de sus productos o servicios entre sus clientes será preciso obtener el consentimiento inequívoco del afectado.

En caso de que una entidad contrate o encomiende a terceros la realización de una determinada campaña publicitaria de sus productos o servicios, encomendándole el tratamiento de determinados datos, se aplicaran las siguientes normas:

- Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por la entidad que contrate la campaña, esta será responsable del tratamiento de los datos.

- Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsables del tratamiento.

-Cuando en las determinaciones de los parámetros intervengan ambas entidades, ambas serán responsables del tratamiento.

4.7 CODIGOS TIPO

Es un documento en el cual, a través de acuerdos sectoriales o mediante decisiones de empresa o convenios administrativos, se establecen las condiciones de organización, el régimen de funcionamiento, los procedimientos aplicables, las normas de seguridad del entorno, la información personal, y las garantías para el ejercicio de los derechos de las personas. También podrán contener reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

Este tipo de documento tiene el carácter de código deontológico o de buena práctica profesional y será vinculante para quienes se adhieran al mismo. Contiene reglas o estándares específicos que permiten armonizar los tratamientos de datos efectuados por los adheridos al código, facilitar el ejercicio de los derechos de los afectados y facilita el cumplimiento de los dispuestos en la LOPD y el Reglamento. Los códigos tipo deben estar redactados en términos claros y accesibles.

La AEPD desea impulsar la elaboración de códigos tipo en aquellos sectores en los que puedan tener mayor relevancia, debido a los factores tales como: la singularidad del sector, la sensibilidad de los datos tratados, la población afectada, las tecnologías utilizadas en el tratamiento de los datos, etc. con el fin de facilitar el cumplimiento de la LOPD y ampliar las garantías ofrecidas al ciudadano en la protección de sus derechos.

Los códigos tipo, que son de carácter voluntario, deben inscribirse en el registro Gral. De Protección de Datos, el cual podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias de la materia. En este último caso el director de la APD indicara las correcciones oportunas que deban efectuar los solicitantes.

Cualquier particular podrá obtener una copia gratuita del código que desee.

4.7.1 CONTENIDO MINIMO DE UN CODIGO TIPO

Los códigos tipo deben respetar la normativa vigente e incluir como mínimo, con suficiente grado de precisión:

* La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.
* Las previsiones específicas para la aplicación de los principios de protección de datos
* El establecimiento de estándares homogéneos para el cumplimiento por los adheridos al código de las obligaciones establecidas en la Ley Orgánica 15/1999 de 13 de diciembre.
* El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición
* La determinación de las cesiones y transferencias internacionales de datos que, en su caso, se prevean con indicación de las garantías que deban adoptarse
* Las acciones formativas en materia de protección de datos dirigidas a quienes los traten, especialmente en cuanto a su relación con los afectados
* Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código tipi
* Clausulas tipo para la obtención del consentimiento de los afectado al tratamiento o cesión de sus datos
* Clausulas tipo para informar a los afectado del tratamiento, cuando los datos no sean obtenidos de los mismos

4.8 LA AUDITORIA

Según el art 17 del Reglamento de seguridad, mediante la auditoria interna o externa se verificará que los sistemas de información y las instalaciones de tratamiento de datos de nivel medio y alto cumplen con el Reglamento de Medidas de Seguridad

Funciones de la Auditoria:

* Adecuar las medidas y controles al Reglamento de Seguridad
* Identificar sus deficiencias y proponer las posibles medidas correctoras
* Incluir los datos, hechos y observaciones en que se basen las decisiones alcanzadas y recomendaciones propuestas

El responsable de seguridad analizara el informe de auditoría, y entregara las conclusiones a las que llegue el responsable del fichero para que adopte las medidas correctoras pertinentes

La auditoría de protección de datos se realizará al menos cada dos años. Además, deberá estar siempre a disposición de la APD

5.EL DOCUMENTO DE SEGURIDAD

5.1 LA SEGURIDAD DE LOS DATOS

Según el art 9 de la LOPD, “el Responsable del fichero, y en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, perdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a los que están expuestos, ya provengan de la acción humana o del medio físico o natural”. Esto quiere decir que no se pueden registrar datos de carácter personal en ficheros que no reúnan las condiciones establecidas por vía reglamentaria con respecto a su integridad y seguridad y, por supuesto, también a la de los centros de tratamiento, los locales, equipos, sistemas y programas.

5.2 EL DOCUMENTO DE SEGURIDAD

Las empresas, ya sean personas físicas o jurídicas, públicas o privadas, que utilicen ficheros automatizados que contengan datos de carácter personal deben elaborar el documento de seguridad. Este documento lo elabora el responsable del fichero y debe contener la normativa de seguridad que se va a implantar en la empresa. Es decir, en el documento de seguridad se redactan todas las medidas técnicas y de organización que se van a adoptar en la empresa para garantizar las medidas de seguridad que han de reunir los ficheros automatizados, los equipos, los programas, las personas, los locales, etc.

Se podrá redactar un único documento de seguridad para todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendría el carácter de documento interno de la organización.

Ahora bien, dependiendo del tipo de datos que contengan los ficheros, las empresas deberán cumplir una cantidad mayor o menor de requisitos para garantizar la confidencialidad y la integridad de esa información. Por lo tanto, el nivel de seguridad que debemos aplicar al documento de seguridad variara dependiendo de cuál sea la naturaleza de los datos.

5.3 NIVELES DE SEGURIDAD DE LOS DATOS

Existen 3, según se especifica en el art 81 del Reglamento

5.3.1 NIVEL BASICO

Se aplica a los ficheros que incluyan datos de carácter personal. Ej: Nombre, apellidos, dirección etc.

5.3.2 NIVEL MEDIO

Deberan implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medios, en:

* Relativos a la comisión de infracciones administrativas o penales
* Aquellos cuyo funcinamiento se rija por el art. 29 de la Ley Organica 15/1999 del 13 de Diciembre (Prestacion de servicios sobre solvencia patrimonial y crédito)
* Ficheros cuyos responsables sean la Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias
* Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros
* Aquellos de los que sean responsables las Entidades, Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social
* Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permiten evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.
* Ej: Info de servicios financieros, seguros y planes de seguros, etc.

5.3.3 NIVEL ALTO

Ademas de las medidas de nivel básico y medios, se aplicaran las medidas de seguridad de nivel alto a los ficheros que contengan datos relativos a la ideología, religión, origen racial, salud o vida secual, a los datos que hayan sido recabados para fines policiales sin el consentimiento de la persona afectada y los ficheros que contengan datos derivados de actos de violencia de genero.

A los datos de trafico y de localización que traten los operadores de servicios de comunicaciones electronicas o de explotación de redes publicas, se les aplicara, además del nivel de seguridad básico y medio, las medidas de nivel alto, contenidas en el art 103 del Reglamento.

Existen varios casos a los cuales se podrá aplicar medidas de nivel básico a ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual:

* Que 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.
* Que 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

Tambien podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o a la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos

5.4 CONTENIDO MINIMO DE LOS DOCUMENTOS DE SEGURIDAD

5.4.1 DOCUMENTO DE SEGURIDAD DE NIVEL BASICO

Contenido es el siguiente:

* AMBITO DE APLICACIÓN DEL DOCUMENTO. En este apartado se deberá especificar el fichero o los ficheros que están bajo el ámbito de aplicación del documento especificando con detalle los recursos que estarán protegidos.
* MEDIDAS, NORMAS, PROCEDIMIENTOS Y ESTANDARES ENCAMINADOS A GARANTIZAR EL NIVEL DE SEGURIDAD EXIGIDO. Este apartado se refiere a las medidas que el responsable del fichero piensa aplicar para hacer cumplir las medidas de seguridad exigidas. Es decir, en este apartado se enumeran todas las medidas y procedimientos que se van a llevar a cabo, en la practica para adoptar las medidas que exige el Reglamento de Seguridad:
* Control de Acceso: Los usuarios tendrán acceso únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. El responsable del fichero se encargara de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos. Solo el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos,

El responsable del fichero establecera mecanismos para evitar que un usuario pueda acceder a recursos a los que no este autorizado.

En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

* Gestion de soportes y documentos: Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ellos en el documento de seguridad. Cuando las características físicas del soporte imposibiliten su identificación o inventariado no se aplicara la medida de seguridad anterior. Sin embargo, deberá quedar constancia motivada de ello en el documento de seguridad.

La identificación de los soportes que contengan datos de carácter personal que la organización cosniderase sensibles se piodra realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citado soportes y documentos identificar su contenido y qu dificulten la identificación por personas no autorizadas.

En cuanto a los soportes no automatizados, el archivo de los mismos se realizara de acuerdo con lo criterios previstos en su respectiva legislación, los cuales deberán garantizar la correcta conservación de los documentos, la localización y consulta de informacio y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. Si no existiera normativa aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación quye deban seguirse para el archivo.

Ademas los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.

Cuando las características ficiscas de quellos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptara medidas que impidan el acceso de personas no autorizadas. Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el articulo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por personas no autorizadas.

* Entrada y salida de soportes: La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendido y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá será autorizada por el responsable del ficghero o encontrarse debidamente autorizada en el documento de seguridad.

En el traslado de la documentación se adoptaran las medidas dirigidas a evitar la sutraccion, perdida o acceso indebido a la información durante su transporte.

* Destruccion de soportes: Siempre que vaya a desecharse cualquier documento o sopote que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterios.
* Identificacion y Autenticacion: El responsbale del fichero o tratamiento adoptara las medidas que garanticen la correcta identificación y autentificación de los usuarios autorizados.

El responsable del fichero o tratamiento establecera un mecanismo que permita la identificacionde forma inquivoca y personalizada de tdo aquel usuario que intente acceder al sistema de información y de verificación de que esta autorizado.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

Las contraseñas deberán cambiarse periódicamente. No podrán mantenerse las mismas contraseñas durante un periodo superior a un año. Las contraseñas, mientras esten vigentes, se almacenaran de forma ininteligible.

* Funciones y obligaciones del personal: El personal que tenga acceso a los datos de carácter personal debe ser informado por el responsable del fichero sobre las normas de seguridad que afecten al desarrollo de sus funciones. Estas funciones y boligaciones estarán claramente definidas en el documento de seguridad.
* EstructURA DE LOS FICHEROS CON DATOS PERSONALES Y DESCRIPCION DE LOS SISTEMAS DE INFORMACION QUE LOS TRATAN. En este apartado se especifica la composición interna de cada fichero (campos y registros incluidos en cada uno) además de la descripción del contenido de los ficheros, soportes y equipos que se hayan utilizado para el almacenamiento y tratamiento de los datos.
* PROCEDIMIENTO DE NOTIFICACION, GESTION Y RESPUESTA DE INCIDENCIAS. Se considera una incidencia cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Se deberá llevar un registro de las incidencias que constara de:

-Tipo de incidencia

-Momento en que se ha producido

-Persona que realiza la notificacion

-Persona a la cual se notifica la incidencia

-Efectos que se hubieran derivado de la incidencia

-Medidas correctoras

* PROCEDIMIENTOS DE REALIZACION DE COPIAS DE RESPALDO Y RECUPERACION DE DATOS EN LOS FICHEROS O TRATAMIENTOS AUTOMATIZADOS.

6. LOS FICHEROS DE TITULARIDAD PUBLICA

6.1 LOS FICHERO DE TITULARIDAD PUBLICA

Los ficheros de titularidad pública, a diferencia de los de titularidad privada, se crean, modifican o suprimen por medio de disposición general que se publica en el BOE o en el diario oficial correspondiente.

Las Admón. publicas no pueden comunicar datos de carácter personal que hayan recogido o elaborado para el desempeño de sus atribuciones a otras Admón. Publicas para el ejercicio de competencias diferentes o que versen sobre materias distintas.

Existen algunas excepciones a los derechos de acceso, rectificación y cancelación en el caso de los ficheros de titularidad pública.

-Los responsables de los ficheros que contengan datos de carácter personal especialmente protegidos, recogidos y tratados con fines policiales por las Fuerzas y Cuerpos de Seguridad, podrán denegar el acceso, rectificación o cancelación, en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades e erceros o las necesidades de las investigaciones que se estén realizando.

-Los responsables de los ficheros de la Hacienda Pública podrán, de igual forma, denegar el ejercicio de los derechos citados cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y en todo caso cuando el afectado está siendo objeto de actuaciones inspectoras.

Las personas a las que se denieguen estos derechos podrán ponerlo en conocimiento del director de la APD o del Organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpo de Policía propios de estas o por Administraciones Tributarias Autonómicas, las cuales deberán asegurarse de la procedencia o improcedencia de la denegación

9- LA AGENCIA DE PROTECCION DE DATOS

9.1 LA AGENCIA ESPAÑOLA DE PROTECCION DE DATOS

La APD es un Ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia de las Admón. Publicas en el ejercicio de sus funciones, que son:

* Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, especialmente en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
* Atender las peticiones y reclamaciones de los afectados, informarles de sus derechos y promover campañas de difusión a través de los medios.
* Controlar a quienes tratan datos.
* Elaborar normas
* Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas
* Velar por la publicidad de los tratamientos.
* Etc.

Forman parte de la estructura de la APD:

* El director
* El Consejo Consultivo
* El Registro General de Protección de Datos
* La Inspección de Datos
* La Secretaria General de la Agencia

El director de la APD ostenta la representación de la Agencia y la dirige. Es nombrado de entre quienes componen el Consejo Consultivo, que emite informes sobre todas las cuestiones que solicite el Director y formula propuestas en materia de protección de datos. Se reúne como mínimo cada 6 meses.

El Registro General de Protección de Datos vela por la publicidad de los tratamientos de datos. Es decir, su principal función es la inscripción de los ficheros de titularidad tanto privada como publica.

La Inspección de Datos se encarga de comprobar la legalidad de los tratamientos y la Secretaria General es un apoyo para el funcionamiento de la Agencia.

9.2 LA PAGINA WEB DE LA AGENCIA DE PROTECCION DE DATOS

La APD pone a disposición de todos los usuarios una web: [www.AGPD.es](http://www.AGPD.es)

En ella pueden consultar sus dudas los empresarios que quieran aclarar cualquier cuestión de materia de protección de datos, y también los afectados que quieran conocer cuáles son sus derechos.

También se puede consultar el Registro General de la Agencia Española de Protección de Datos, en el cual se encuentran inscritos los ficheros de las empresas de todo el país.

También hay una sección de Actualidad donde se pueden leer las últimas novedades sobre protección de datos.

10.RECAPITULACIONES

10.1 ¿Qué ES LA LOPD?

Es una Ley, aprobada en 1999, cuyo objeto es la protección de datos personales, un derecho fundamental de las personas físicas al honor y la intimidad personal y familiar. La LOPD entro en vigor el 14 de enero de 2000 para los ficheros automatizados. Para los ficheros que no están automatizados esta Ley se comenzó a aplicar el 24 de octubre de 2007.

10.2¿Por qué SE DEBE APLICAR LA LOPD?

Por varios motivos: El más importante es para cumplir con el derecho fundamental de las personas a la intimidad al honor recogida en la Constitución art. 18. Con el cumplimiento de la LOPD, la empresa da una imagen de respeto por la intimidad del cliente.

Otro motivo es evitar sanciones de hasta 600.000 €.

10.3¿QUE REQUISITOS HAY QUE LLEVAR A CABO PARA CUMPLIR LA LOPD?

* Inscripción de los ficheros en el Registro General de Protección de Datos
* Elaboración del Documento de Seguridad
* Comunicación del Documento de Seguridad a los distintos miembros de la empresa.
* Elaboración de los distintos documentos de solicitud de acceso, cancelación, rectificación, oposición y derecho de información.

Dependiendo del tipo de datos que trate la empresa variaran las medidas de protección que haya que tomar