LEY DE PROTECCION DE DATOS

ERSM
Insurance Brokers
Crèdit Andorrà Financial Group

1 de abril de 2018

INDICE

OBJETIVO DEL CURSO

El objetivo del curso que nos ocupa, es adquirir los conocimientos necesarios para nuestro puesto de trabajo en relación a la protección de los datos personales, en concreto:

- A identificar los hábitos de trabajo correctos en el tratamiento de los datos personales
- Aprender los conceptos relacionados con la normativa de protección de los datos.
- Conocer las consecuencias que de un mal uso de los datos personales pueden derivarse.

Para la realización del curso no son necesarios conocimientos previos, si bien a la finalización del mismo debería disponerse del conocimiento necesario para interpretar correctamente el documento de seguridad existente en la empresa, el cual debe seguirse conforme a las directrices proporcionadas por la misma

.

UN DERECHO FUNDAMENTAL

Las necesidades de las empresas y profesionales de minimizar los esfuerzos en el proceso de la información y el avance en las tecnologías de la información, han llevado a la **proliferación de bases de datos y ficheros de los que nuestros datos son el alimento fundamental**.

La informatización de dichos ficheros no siempre se ha realizado adoptando las medidas de seguridad necesarias y son cada vez más los datos que sobre nuestra vida, nuestra salud, nuestros hábitos, que se encuentran dispersos o agrupados en multitud de ficheros. No es vana la imagen que la ciencia ficción nos propone, en la que la vida de un ser humano puede ser modificada a través de cambios en los ficheros en los que constan sus datos personales, no es ninguna obviedad el hecho de que determinadas personas han debido recorrer un largo camino para corregir los errores que en ficheros de carácter administrativo se han producido.

Sirva de ejemplo de la necesidad de esta normativa, el conocido caso de cesión de datos realizado por Facebook con motivo de las elecciones americanas a la empresa Cambridge Analytics al objeto de influir en las votaciones de los usuarios en función de la información existente en Facebook

Conscientes de esta realidad y al objeto de proteger a los ciudadanos, tanto a nivel nacional como a nivel comunitario se ha desarrollado la normativa que regula el tratamiento de los datos

La Constitución española ya reconoce el derecho de los ciudadanos a la protección de sus datos y es el Título I sobre los derechos y deberes fundamentales, en su capítulo segundo de derechos y libertades en la sección 1ª, en su artículo 18, donde en su punto cuarto encontramos el siguiente redactado:

> *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."*

La Ley Orgánica 15/1999 de 13 de diciembre **desarrolla el precepto constitucional** del artículo 18.4. lo que es un indicativo de la importancia de esta ley

A nivel comunitario la protección de datos queda regulada en el **Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016**, reglamento que en España entra en vigor el 25 de mayo de 2018. Este reglamento es de obligado cumplimiento para todos los países de la CCEE y tiene como principal objetivo unificar el tratamiento de la protección de datos en los diferentes países de la CEE, ya que con anterioridad al mismo existían diferentes regulaciones, con diferentes niveles de exigencia. Este reglamento unifica y armoniza la legislación en materia de protección de datos en los diferentes países de la CCEE

Concepto de dato personal

Los **datos personales** son **todos aquellos que se asocian a las personas físicas**.

Los datos están vinculados a una *persona identificable*, de esta manera para que un dato personal deba ser tratado conforme a los principios de protección de datos, debe poder identificarse la persona física a la que corresponden los datos, bien directa o indirectamente.

En base a este criterio, las estadísticas de población en las que no es posible identificar las personas exactas a las que respondan, no tendrán la consideración de datos personales.

El punto anterior no sería cierto si a través de cruce con otros ficheros pudiésemos identificar las personas a partir de las que se han generado las estadísticas.

Es obligación de todas las personas y empresas con acceso a datos personales realizar el **tratamiento** de los mismos de manera **que se preserven los derechos del titular de la información**, garantizando su intimidad.

La intimidad no solo afecta a los datos que podríamos considerar más sensibles, sino a la totalidad de los datos que hacen referencia a las personas.

En relación a los datos personales, la legislación sobre Protección de datos, tiene como uno de sus objetivos evitar que el cúmulo de información de una persona, como consecuencia de un uso indebido de la información, nos proporcione un perfil amplio que afecte a los límites de su intimidad.

Concepto de protección de datos

El principio de protección de datos consagra el **derecho de las personas físicas a decidir sobre el uso de sus datos personales**.

Si bien tradicionalmente este concepto se ha asociado al tratamiento automatizado de los datos, no es cierta esta afirmación, pues no solo **los ficheros informáticos deben ser objeto de protección**, sino **también los ficheros en papel**, en los que igualmente se conservan datos de las personas.

A efectos de la normativa de protección de datos se define el **tratamiento** como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

A tenor de la definición anterior la protección de datos no se limita al tratamiento automatizado, sino a cualquier forma, soporte o uso que se realice de los datos, incluyen la destrucción de los mismos

El principio de protección de datos avala el derecho a la intimidad en el sentido más amplio, en el sentido de que cualquier dato de la persona debe ser objeto del tratamiento según los criterios marcados por la Legislación de protección de datos.

El principio de protección de datos tiene por objeto **garantizar que solo el titular de los datos puede decidir sobre el uso de la información, así como sobre las personas o empresas que tienen acceso a los mismos**.

Si la persona es la única con capacidad para decidir sobre sus datos, un nuevo principio se consagra y hace referencia la cesión de los datos, cesión que no se puede hacer, sin la expresa autorización del titular de los datos.

El tratamiento de los datos por parte de las empresas o de los profesionales **debe venir establecido por un contrato, acuerdo, convenio o relación mercantil o laboral** y será el marco del acuerdo entre el titular de los datos y la empresa o profesional, el que determine el tratamiento de los datos que puede realizarse.

La legislación de protección de datos sobre todo pone límites al tratamiento de los datos por parte de las empresas y profesionales con el fin de que los mismos se ajusten al mandato otorgado por el titular de los datos.

Esta relación contractual que se establece entre el titular de los datos y la empresa debe ser conocida por ambas partes, siendo conocida igualmente la existencia del fichero en el cual se incorporarán los datos objeto de tratamiento y la finalidad del mismo.

El mandato otorgado por el titular de los datos debe ser tenido en consideración hasta sus últimas consecuencias, ello supone, que incluso si un familiar o un amigo nos proporcionan la información en el marco de una relación profesional, nunca podremos hacer uso de la información en el ámbito personal.

Supongamos que un familiar o un amigo nos viene a solicitar al despacho profesional y nos solicita la prestación de un servicio o un producto (ej. a contratar un seguro, a pedir precio para un coche o cualquier otra gestión), bajo ningún concepto podremos comunicar a otros familiares o amigos la información que hemos obtenido en la gestión profesional. Si por el contrario está información nos la proporciona en el ámbito personal, esto es cuando estamos charlando tranquilamente fuera del despacho profesional, quedará dentro del marco de la discreción de cada uno el comunicar esta información a terceras personas, dado que la información queda fuera del ámbito profesional.

La **cesión de datos** queda especialmente marcada por este principio de protección de datos, la cesión de datos solo será posible en los casos en que:

- Venga **establecida por alguna ley**, como es el caso de las declaraciones de impuestos, así cederemos a la administración pública los datos sobre las retenciones ejercidas en las nóminas de los trabajadores o los datos de seguridad social, igualmente sucede con las entidades aseguradoras cuando los datos son trasladados por un corredor de seguros

- Sea **requerido por vía judicial**

- Tengamos la **autorización o el mandato del titular de los datos** y dicha cesión sea conocida por el mismo, como es la cesión de los datos a las entidades aseguradoras destinatarias de los contratos.

Hay **situaciones** que tradicionalmente vienen produciéndose y **que deben ser corregidas** en base a los principios de la protección de datos, siendo algunos ejemplos:

- **Proporcionar documentación o información a familiares del titular sin que exista autorización** expresa del titular. Esta situación que ha sido una realidad durante mucho tiempo debe ser corregida solicitando al titular autorización expresa para proporcionar información a terceras personas, debiendo concretarse de forma inequívoca las personas a las que se puede proporcionar la información

- **Petición de entidades que realizan otras gestiones para el titular de los datos** como puede ser los datos proporcionados en caso de siniestro a contrarios, en este caso solo podremos proporcionar esta información en el caso en que nuestro asegurado nos haya informado previamente del siniestro y nos haya autorizado a su tramitación. En caso de que se nos informe de la participación de nuestro asegurado en un siniestro, primero deberemos confirmarlo con el mismo previamente a proporcionar información y una vez obtengamos la confirmación, solo proporcionaremos la información que se precise para la tramitación del siniestro, nunca información que no sea necesaria. Lo mismo sucedería con peticiones de información a gestorías relativas a facturas de clientes, si un tercero nos solicita información contable sobre facturas de un autónomo, únicamente podríamos proporcionarla en el caso en que el mismo nos autorizará

NORMATIVA DE PROTECCION DE DATOS

La normativa sobre protección de datos **nace en la propia constitución**, es el Título I sobre los derechos y deberes fundamentales, en su capítulo segundo de derechos y libertades en la sección 1ª, en su artículo 18, donde en su punto cuarto encontramos el siguiente redactado:

> *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."*

A partir del precepto proporcionado por la constitución, se desarrollan diferentes tipos de normas que en todo caso serán de obligado cumplimiento, las normas las podemos dividir en:

- Normas generales
- Instrucciones de la Agencia de Protección de datos
- Normativa europea

Normas generales

Las normas generales actualmente en vigor son:

- Ley orgánica 15/1999 de Protección de datos de carácter personal (LOPD)

  Esta ley desarrolla el precepto marcado por la constitución y en la que se reconocen los derechos de los ciudadanos en relación al tratamiento de sus datos personales.

  Se establecen por una parte las garantías para los titulares de los datos, al tiempo que se establecen las obligaciones para las empresas que los tratan.

  Es la norma de rango superior por el que se rige el tratamiento de los datos personales y tiene como finalidad no solo garantizar el tratamiento de los datos

personales, sino que también debe permitir al titular de los datos verificar el cumplimiento de sus derechos.

- Real decreto 1332/94 de 20 de junio por el que se desarrollan algunos preceptos de la Ley Orgánica

  Puede sorprender que este real decreto sea anterior a la Ley Orgánica, pero la realidad es que este Real Decreto desarrolla la anterior Ley orgánica, de 5/92 de 29 de octubre.

  Este reglamente no queda derogada por la posterior ley 15/1999 al no haber sido desarrollado el reglamento exigido por la misma, por lo que los preceptos establecidos en el reglamente y basados en la anterior ley orgánica anterior siguen siendo de aplicación.

  En este reglamento se establecen algunas definiciones que continúan siendo vigentes, así como se concretan diferentes aspectos respecto a los derechos de los titulares de los datos o se establecen los criterios para las transferencias internacionales de datos

- Real decreto 994/1999 de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros automatizados que contengan datos de Carácter Personal

  Tras la Ley Orgánica 15/99 se desarrollará este reglamente en el que se establecen las medidas que han de adoptar las empresas en los ficheros automatizados, convirtiéndose en un marco de referencia a la hora de implantar y desarrollar sistemas de información.

  Hasta la fecha este reglamento es el que mayor impacto ha tenido en la implantación de la protección de datos en las empresas, al obligar en muchos casos en las empresas a la adecuación tanto de las aplicaciones como de los procedimientos de uso de las mismas por parte de los usuarios.

  Este reglamento afecta únicamente a los ficheros automatizados, quedando pendientes de desarrollo las medidas para los ficheros en papel.

Este reglamente establece diferentes medidas en función de la naturaleza de los datos a proteger, siendo las medidas más exigentes cuando los ficheros contengan información catalogada por la Ley como información confidencial y las menos exigentes para el caso en que los ficheros únicamente contengan datos personales catalogados como protegidos.

Instrucciones de la agencia de protección de datos

Las instrucciones de la agencia de protección de datos tienen como objetivo concretar o aclarar determinados artículos de la ley o dar respuesta a situaciones que pudieran ser objeto de discusión.

Las instrucciones hasta la fecha publicadas por la agencia de protección de datos son:

- Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito.

  Hace referencia a las condiciones que deben darse para inscribir a una persona en ficheros de impagados y similares, así como las medidas excepcionales de aplicación a los mismos.

- Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal.

  Esta resolución establece los requisitos que han de seguirse desde el punto de vista de protección de datos para la contratación de un seguro de vida, conjuntamente con un préstamo hipotecario.

  Esta instrucción busca sobre todo la claridad en relación a la protección de datos en este tipo de operaciones, estableciendo que el cliente en todo momento debe conocer quién es el destinatario de los datos tanto de la operación crediticia como de la aseguradora, debiendo igualmente proporcionarse la información al cliente de las empresas en las que puede ejercer sus derechos en cada uno de los casos y finalmente debe recogerse la información en documentos diferenciados.

- Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.

  Esta instrucción establece que el control automatizado del acceso a los edificios tendrá la consideración de un fichero a proteger conforme a los criterios de protección de datos y que los datos únicamente pueden usarse con esta finalidad.

- Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.

- Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

  Esta instrucción nos proporciona las pautas para el ejercicio de los derechos que asisten a los titulares de los datos, estableciendo la manera en que los mismos pueden ejercerse y los requisitos que deben cumplirse.

- Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección, relativa a las normas por las que se rigen los movimientos internacionales de datos

  El objetivo de esta instrucción es garantizar que los países destinatarios de los datos tengan las mismas exigencias de protección de datos que las que tiene España.

  Entre otros aspectos, se establece que los países a los que se realicen transferencias deben estar expresamente autorizados por la agencia de protección de datos.

- Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus resoluciones

- INSTRUCCIÓN 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

  En la existencia de la video vigilancia en las empresas, esta instrucción nos proporciona las directrices tanto para el registro del fichero, como para informar a las personas objeto de grabación de la existencia del sistema de video vigilancia.

<u>Normativa Europea</u>

La normativa europea tiene como objeto unificar los criterios de protección de datos en todos los países de la CEE y son de obligado cumplimiento para todos los países miembros:

- Carta de los derechos fundamentales de la Unión Europea

  En sus artículos 7 y 8 establecen respectivamente como derechos fundamentales de los ciudadanos de la comunidad económica europea el respeto a la vida privada y familiar y la protección de datos personales

- Directivas que recogen aspectos específicos relativos a la protección de datos , entre otros al tratamiento de las redes sociales y comunicaciones

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

  Este reglamento entra en vigor en España el 25 de mayo de 2018 y es de obligado cumplimiento para todos los países de la CEE a partir de esta fecha. Sobre el mismo podrán realizarse desarrollos en los diferentes países que amplíen o desarrollen los preceptos del mismo.

CONCEPTOS Y DEFINICIONES

Las diferentes normas y reglamentos nos proporcionan múltiples definiciones en relación a la Ley de Protección de Datos, conceptos que vamos a repasar:

- Datos de carácter personal:

  Cualquier información concerniente a personas físicas identificadas o identificables.

  Esta definición nos proporciona dos elementos clave, el primero es que la Ley de Protección de datos **solo es de aplicación a las personas físicas**, excluyendo por tanto a las personas jurídicas. La exclusión de las personas jurídicas no afecta a las personas físicas de las que se tenga información a través de las personas jurídicas, cuya información debe ser igualmente tratada conforme a los criterios de la ley de protección de datos

  El segundo elemento destacable es que los datos para tener el carácter de datos personales deben corresponder a una persona física **identificada o identificable**. No serán por tanto datos personales las estadísticas de carácter general en las que no es posible identificar las personas físicas a las que hacen referencia, por tanto siempre que los datos no estén vinculados a ninguna persona, no será necesario actuar conforme a los criterios de protección de datos.

- Fichero:

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

  El concepto de fichero que nos proporciona la ley establece que sea cual sea el soporte en el que se encuentren los datos, siempre que los mismos sean datos organizados tendrán la consideración de ficheros. Es por tanto erróneo que los ficheros en papel no se vean sometidos a los principios de protección de datos,

que claramente en función de la definición que la Ley nos proporciona sobre fichero, quedan sometidos a los principios de protección de datos.

- **Tratamiento de datos:**

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

  Cualquier procedimiento de datos, tenga que ver o no con la existencia de un fichero, queda sometido al principio de protección de datos, según esta definición. El tratamiento de los datos definido contempla las diferentes fases, entendiendo el tratamiento desde el momento en que los mismos son captados, cualquier proceso intermedio y finalmente su cancelación o destrucción.

  La cesión o transferencia de datos a terceros tienen son igualmente procesos de tratamiento de datos. Esta definición nos sitúa frente a cualquier proceso en el que intervengan datos personales.

  A tenor de la definición que nos proporciona la ley de fichero, no solo debemos considerar tratamiento de datos los procedimientos informáticos, sino también todos los procesos existentes en la empresa en los que tratamos documentos en papel que contengan datos personales.

- Responsable del fichero o tratamiento:

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

  El elemento determinante para establecer el **responsable del fichero** o tratamiento es la **capacidad de decisión sobre el uso, fin o contenido de los datos**, es por ello que la ley distingue entre el **encargado**, que es quien efectivamente **gestiona el fichero** y el responsable, que es el que tiene la capacidad de decisión sobre el fichero.

  La empresa puede externalizar su gestión laboral y fiscal en otra empresa, pero la capacidad de decisión sobre el uso, contenido o finalidad pertenece a la empresa

propietaria de la información, debiendo igualmente velar por el cumplimiento de las normas relativas a protección de datos.

La importancia del establecimiento del responsable del fichero obliga a este a exigir a cualquier encargado en el que delegue la gestión del fichero, el cumplimiento de las normas de protección de datos, obligación que deberá plasmarse en un contrato de tratamiento de datos por cuenta de terceros.

Tendrán por tanto la consideración de encargados de tratamiento servicios como el del asesor fiscal, asesor laboral, la empresa de mantenimiento de la red informática o la empresa de prevención de riesgos laborales entre otros, debiendo establecerse con cada uno de los mismos un contrato de encargo de tratamiento que establezca claramente los datos precisos para la prestación del servicio, la finalidad del tratamiento y la sistemática de actuación con los datos a la finalización del servicio

- Afectado o interesado:

  Persona física titular de los datos que sean objeto del tratamiento

  El afectado o interesado es la persona física a la que hacen referencia los datos personales objetos de tratamiento, esto supone que **es el único que puede ejercer los derechos asociados a la protección de los datos.**

  Cada persona es un afectado o interesado en todos y cada uno de los ficheros en los que existe información sobre la misma, desde que somos niños nuestra información es incorporada a diferentes ficheros, en el colegio, en el hospital, en diferentes registros y en cada uno de los ficheros la persona tiene la consideración de afectado.

  Erróneamente pensamos que son los datos de nuestros clientes los que debemos proteger y si bien es cierto que es de los mismos de quien disponemos de un mayor cúmulo de información, los criterios de protección son igualmente de aplicación a los proveedores que sean personas físicas o cualesquiera otro tipo de personas físicas que figuren en nuestros ficheros.

- Procedimiento de disociación:

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

Cuando los datos tratados pierden el vínculo con la persona física que los genera, es a través de un procedimiento de disociación, **dejando de ser a partir de ese momento un dato personal**.

Cuando se realizan encuestas o entrevistas, en los que no se conserva el nombre o cualquier otro dato identificativo del titular de los datos se están disociando los datos.

Otro ejemplo de procedimiento de disociación que nos proporcionaría un fichero no sujeto a tratamiento de datos personales, es el que se produce cuando de nuestros ficheros obtenemos un segundo fichero en el que se han eliminado cualquiera de los datos que permitan identificar el titular de la información, nombre, NIF, dirección y únicamente pasamos diferentes datos no vinculados a las personas, con los que realizar un análisis de nuestra cartera y no de personas determinables.

- Encargado del tratamiento:

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

El encargado del tratamiento es quien realiza el tratamiento del fichero, pudiendo este coincidir con el responsable del fichero o ser ajeno al mismo, como ya hemos comentado con anterioridad.

Corresponde al responsable del fichero exigir del encargado el cumplimiento de las normas de protección de datos, para lo que deberá proporcionar las directrices de tratamiento y exigir su cumplimiento.

- Consentimiento del interesado:

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

El consentimiento del interesado es una de las exigencias de la Ley Orgánica de Protección de datos, debiendo cumplir que los requisitos de ser:

- **Libre:** lo que supone que no puede existir coacción en el consentimiento, de tal manera que si la coacción se probase, se entendería que el consentimiento no ha sido otorgado, es por ello que siempre que existan contratos vinculados como el de vida y un préstamo hipotecario, el consentimiento a uno de los mismos, debe ser claramente independiente del otro.

- **Inequívoca:** no deben existir dudas respecto al consentimiento otorgado y la finalidad para la que el mismo se otorga, esto nos obliga a ser concretos en los documentos en los que solicitamos al cliente el consentimiento y le informamos de la existencia del fichero y usos a los que el mismo se destina.

- **Específica:** el consentimiento debe otorgarse para un tratamiento de datos concreto y específico. Por lo tanto hemos de ser cuidadosos a la hora de establecer la finalidad del fichero, dado que únicamente podremos utilizar los datos para la finalidad establecida.

- **Informado:** el titular de los datos debe estar perfectamente informado sobre la finalidad a la que se destina el fichero.

Es importante recabar la autorización de los clientes para una finalidad concreta, de forma que esta autorización no se preste a confusión respecto el consentimiento otorgado.

- <u>Cesión o comunicación de datos:</u>

  Toda revelación de datos realizada a una persona distinta del interesado.

  Cualquier transmisión de datos a un tercero diferente de aquel a quien otorgo el consentimiento el titular de los datos, tendrá la consideración de cesión o comunicación de los datos.

  La normativa de protección de datos prohíbe expresamente cualquier cesión o comunicación de datos que no esté amparada por una ley (como es el caso de las

cesiones a la administración pública) o autorizada por el titular (como podría ser las cesiones que rellenamos cuando nos apuntamos a un concurso en el que explícitamente se nos informa de que vamos a ceder nuestros datos a terceras empresas).

El consentimiento para gestionar nuestros datos se concreta para una finalidad y podemos establecer un periodo determinado, pero no es necesario prestarlo cada vez que se concrete la necesidad, Así si prestamos el consentimiento para que trate nuestros datos para realizar compras en una determinada página web, una vez confirmada nuestra autorización, no será necesario con cada acceso confirmarla.

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, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.

Las fuentes accesibles al público marcan aquellos datos de los que podemos mantener en nuestros ficheros, sin que exista una autorización previa del titular de los datos, si bien cualquier ampliación de la información o tratamiento sobre la misma requerirá de la autorización del titular de los datos.

En nuestros ficheros podremos mantener información relativa a ficheros públicos, pero para el tratamiento de los mismos (incluyendo en este el envío de publicidad), requeriremos del consentimiento del afectado.

Es por ello que con frecuencia aparecen páginas web en las que con frecuencia nos solicitan nuestra aceptación para enviarnos promociones y son estas empresas especializadas las que envían promociones de diferentes clientes.

- **Bloqueo de datos:**

  La identificación y reserva de datos con el fin de impedir su tratamiento.

  El bloqueo de datos es el procedimiento mediante el cual, aun conservando los datos en el fichero, estos no pueden ser tratados.

  Este sería el caso de los registros de un fichero marcados a fin de no recibir publicidad a petición expresa de sus titulares, estos registros quedarían marcados impidiendo su proceso en envíos publicitarios.

  El bloqueo de los datos puede ser de diferentes niveles, siendo el bloqueo total, aquel en que ningún usuario puede acceder a los datos, siendo únicamente el responsable de seguridad quien en circunstancias especiales acceda a los datos.

  Los procedimientos de bloqueo de dato deben ser recogidos en el documento de seguridad y tienen como objetivo garantizar el efectivo cumplimiento de los diferentes derechos que la ley otorga a los titulares de los datos personales.

- **Identificación del afectado:**

  Cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada.

  La identificación del afectado **es determinante a la hora de establecer si los datos** en nuestros diferentes **ficheros son o no datos personales**.

  Siempre que exista un procedimiento de identificación del afectado o la naturaleza de los datos permita establecer de la persona física titular de los datos, los mismos tendrán la consideración de datos personales.

  La definición que nos proporciona el reglamento de protección de datos nos sitúa ante una identificación del afectado que no requiere de un exhaustivo conocimiento del titular de los datos, basta con que el análisis de los mismos nos pueda conducir hasta la persona física, tendrán la consideración de datos personales.

- **Transferencia de datos:**

  El transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional.

  La amplitud del concepto de transferencia de datos nos lleva a una revisión de nuestros procesos diarios de trabajo, en los que la transferencia de datos se produce de forma continuada, debiendo esta transferencia quedar sometida a los principios de protección de datos.

  Algunos ejemplos cotidianos de transferencia de datos son el envío documento por mensajero, el envío de un correo electrónico o cualquier otro medio a través del que estemos proporcionando información de personas físicas.

  Lo importante en estos procesos es que la transferencia debe realizarse de acuerdo a la autorización realizado por el titular de los datos, es por ello que en los medios habituales de transmisión de datos hemos de tener siempre en consideración los principios de protección de datos.

  No es infrecuente enviar un correo electrónico a más de un destinatario, envíos en los que al no ocultar las direcciones (si no utilizamos la opción "con copia oculta" estamos transmitiendo datos personales a terceras personas, transmisión que en muchos casos no responde a la autorización proporcionada por el titular de los datos.

- **Sistemas de información:**

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

  La definición anterior nos proporciona un concepto amplio de los sistemas de información, no solo el servidor o los equipos informáticos existentes en la empresa forman el sistema de información, sino **cualquier soporte en el que almacenemos o tratemos datos personales.**

  El abaratamiento de los sistemas de almacenamiento de información y transferencia de archivos, ha llevado a la proliferación de los soportes USB o las

PDA, dispositivos que igualmente forman parte del sistema de información y deben ser controlados a fin de que no se realice un uso indebido de los mismos.

Las empresas no solo tienen la obligación de mantener la seguridad de sus sistemas internos, sino que deben velar por que no se utilicen dispositivos no controlados y no autorizados en los que pudiera hacerse un uso indebido de los datos personales.

No es infrecuente que las empresas protejan sus sistemas mediante complejos sistema de contraseñas, al tiempo que permiten la existencia de PDA, que pueden ser extraviadas y en las que no existen métodos de protección o dispositivos USB a los que se trasladan datos y en los que no existen contraseñas o sistemas de cifrado.

Es importante en este sentido impedir o bien establecer claramente los criterios bajo los que los integrantes de una organización pueden utilizar dispositivos móviles con información de la empresa, aspecto este que en muchas ocasiones no se incorpora al documento de seguridad.

- **Usuario:**

  Sujeto o proceso autorizado para acceder a datos o recursos.

  El usuario será toda persona con autorización para acceder a los datos personales o a los recursos que dan acceso a los mismos. Según este principio deberemos considerar usuario a cualquier persona que tenga accesos a nuestros equipos informáticos, con independencia de los derechos de acceso.

  Adicionalmente se introduce el concepto de usuario en los procesos, ello quiere decir que cuando los datos sean procesados mediante un sistema planificado de ejecución de procesos, debe igualmente identificarse el proceso como un usuario de sistema.

  La importancia de la consideración de usuario de un sistema, es la necesidad de garantizarnos que el uso que se realice de los recursos sea acorde a las instrucciones proporcionadas por la empresa, evitando que el usuario incorpore procedimientos o recursos no autorizados por la empresa.

El usuario tiene como objetivo restringir los accesos en función del perfil asignado por la empresa, además de registrar todos los accesos a los datos sensibles, es por ello que deben eliminarse prácticas como la de comunicar la contraseña a otros usuarios de la empresa. Cada usuario asume las responsabilidades de sus acciones y debe ser identificado de forma única en la empresa.

- Recurso:

  Cualquier parte componente de un sistema de información.

  Entenderemos como recurso todos los elementos, sean de la naturaleza que sean que forman parte del sistema de información, por tanto no solo el disco, la memoria, sino incluso el papel deben considerarse parte del sistema de información y por tanto debe ser tratado con las precauciones debidas.

- Accesos autorizados:

  Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

  Los accesos autorizados son aquellos que vienen autorizados por la empresa y para los que se han definido las diferentes políticas de seguridad

  El concepto de acceso autorizado nos conduce hasta su opuesto, siendo estos los accesos no autorizados, aquellos que se producen en los sistemas de información y no han sido autorizados por el administrador del sistema, son por tanto los accesos que deben ser evitados mediante el establecimiento de las medidas de seguridad.

  Las autorizaciones de usuario en los sistemas informatizados vienen marcadas por los perfiles de acceso que otorgan los programas o los accesos a servidores y ordenadores de la empresa, pero es igualmente necesario establecer las autorizaciones en papel, implantando las medidas que eviten el acceso no autorizado a documentación en papel.

  Ello supone que los archivos deben estar protegidos en armarios o lugares protegidos y su acceso controlado por personas autorizadas.

Si un armario dispone de llave, pero la misma siempre está puesta, no estaremos evitando los accesos no deseados, la llave debería estar en poder de uno o más usuarios autorizados, que dispongan así mismo de la relación de los restantes usuarios autorizados, siendo quienes disponen de la llave del control de los accesos.

Para los datos sensibles, la legislación establece no solo que los accesos deben estar controlados, sino también registrados, ello supone que siempre que un usuario acceda a un expediente en papel con datos sensibles, debe dejar constancia en un registro, indicando el expediente, el motivo y la fecha en que coge el expediente y la fecha en que el mismo es reintegrado a su lugar de custodia.

- <u>Identificación:</u>

  Procedimiento de reconocimiento de la identidad de un usuario.

  La contraseña por sí misma no conforma la identificación, el procedimiento de reconocimiento de la identidad de un usuario, el procedimiento lo constituyen todos y cada uno de los procesos que los sistemas realizar para identificar el usuario.

- <u>Autenticación:</u>

  Procedimiento de comprobación de la identidad de un usuario.

  Serían los procesos que mantienen los programas y sistemas operativos para identificar el usuario que accede a los datos, así como los accesos a la información existente en los ficheros.

- <u>Control de acceso:</u>

  Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

  Los mecanismos de control nos permiten establecer cuáles son los accesos permitidos a los usuarios, es el conjunto de reglas que permiten establecer quién

es el usuario, a que datos y transacciones está autorizado a gestionar / Consultaar

- **Contraseña:**

  I*nformación confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.*

  Respecto a la contraseña los sistemas deben atender las exigencias marcadas por el Reglamento de medidas de seguridad, cuales son:

  - Mantener un grado de **complejidad** que dificulte a terceras personas utilizar la misma.
  - **Privada:** Nunca debe ser proporcionada a otros usuarios o personas
  - Debe ser **modificada** con la periodicidad que la empresa establezca.
  - Debe ser **obligatoria** para el acceso a todos los ficheros en los que existan datos personales.

- **Incidencia:**

  Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

  Desde la existencia de un virus, a la perdida de información como consecuencia de un fallo en el sistema deben ser consideradas incidencias de seguridad, tanto los accesos no autorizados como las posibles pérdidas de información, deben ser evitados en el diseño de los sistemas de información.

  El responsable de seguridad deberá mantener el registro de todas las incidencias que se produzcan, así como identificar las consecuencias de las mismas y las medidas que se han adoptado para evitar que se produzcan de nuevo.

  La legislación vigente establece la obligación de notificar a los afectados las incidencias de seguridad siempre que pueda afectar a sus derechos u libertades

- **Soporte:**

Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

Los Pen Drive, discos externos o internos, PDA, teléfonos o cualquier otro dispositivo en el que se pueda conservar o transportar información tendrá la consideración de soporte y por tanto debe ser controlado por la empresa

- 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.

Toda empresa o profesional con ficheros con datos personales deberá establecer quién es el responsable de la implementación de las medidas que garanticen que no se producen usos indebidos de la información.

- Copia del respaldo:

Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

La copia de respaldo o seguridad tiene como finalidad que el responsable de los ficheros garantice que los datos están preservados de posibles pérdidas de información.

La Ley de protección de Datos no solo obliga a garantizar el correcto tratamiento de los datos, sino a que la información se preserve de igual manera.

Adicionalmente y respecto a las copias de seguridad, dado que generalmente se realizan en servidores remotos o dispositivos móviles, las mismas deben realizarse de forma cifrada, evitando con ello que si alguien se hace con las copias de seguridad, haga un uso indebido de la información.

LOS PRINCIPIOS DE PROTECCIÓN DE DATOS

Los principios que todas las empresas deben tener en consideración a la hora de tratar datos personales se concretan en:

1. El consentimiento del titular de los datos

   El mantenimiento de datos personales en la empresa requiere la autorización del titular de los datos y los mismos deben ser utilizados exclusivamente para el fin o fines que ha autorizado el titular.

   Una pregunta que se plantea con frecuencia a quienes mantienen datos personales en sus ficheros profesionales o de empresa es: ¿En qué circunstancias la Ley me obliga a solicitar el consentimiento de los interesados?

   La respuesta en muchas ocasiones es desconocida por el empresario y, sin embargo, **las consecuencias de no disponer del consentimiento del interesado en los datos personales existentes en los ficheros son importantes**, ya que el incumplimiento de lo dispuesto en la LOPD puede acarrear sanciones que pueden llegar a los 10.000.000 € o al 2% de la facturación de la empresa y respuesta es siempre

   ¿Cuál es el criterio que establece la Normativa Europea para la obtención del consentimiento?

   El artículo 7º establece con claridad que para el tratamiento de los datos de carácter personal se exige el **consentimiento "inequívoco"** del interesado, salvo que la ley disponga otra cosa e igualmente establece que el responsable deberá ser capaz de demostrar que el interesado consintió el tratamiento de los datos personales

   El consentimiento inequívoco es aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa.

   El consentimiento libre, informado, específico e inequívoco del interesado y se contemplan situaciones en las que el **consentimiento**, además de inequívoco, ha de ser **explícito,** siendo estas:

- Tratamiento de datos sensibles, tanto por categorías de datos definidas como tales (los referidos a la ideología, afiliación sindical, religión y creencias) o bien cuando existe un nivel de datos elevado
- Adopción de decisiones automatizadas, cuando a partir de los datos se adopten decisiones automatizadas que afecten a los interesados en base a la creación de perfiles específicos
- Transferencias internacionales, entendiendo como tales las que se realicen a países ajenos a los miembros de la CEE y que no hayan sido aceptados como países asimilados.

El consentimiento **puede** ser inequívoco y **otorgarse de forma implícita** cuando se deduzca de una acción del interesado (por ejemplo, cuando el interesado continúa navegando por una web y acepta así el que se utilicen cookies para monitorizar su navegación).

Los **tratamientos iniciados con anterioridad** al inicio de la aplicación del reglamento europeo sobre la base del consentimiento seguirán siendo legítimos siempre que ese consentimiento se hubiera prestado del modo en que prevé la legislación, es decir, mediante una manifestación o acción afirmativa o bien exista una base legal que legitime su tratamiento

Cuando obtenemos el consentimiento “implícito” del afectado

El consentimiento **"implico"** es aquel que **se deduce de nuestros propios actos**, aunque no haya habido una conducta expresa en tal sentido. Ejemplo de ello sería el caso en el que el cliente nos proporciona su información a través de un formulario en una página web. Si en la página web estamos informando de la existencia del fichero, el internauta al rellenar el formulario de la web, a pesar de no haber declarado en ningún momento que autoriza el tratamiento y cesión de sus datos, si en la propia página le informamos de:

1. La existencia de un fichero de destino para sus datos;
2. La finalidad del mismo
3. Los posibles destinatarios;

4. Del carácter obligatorio o facultativo de las respuestas que proporcione

5. De la forma y ante quien puede ejercer los llamados derechos de acceso, rectificación, cancelación y oposición a los mismos.

En este caso el presunto consentimiento será en este caso aceptable conforme a los criterios establecidos por la normativa, siempre y cuando previamente al envío del formulario el cliente haya afirmado haber leído y aceptado la política en materia de protección de datos, no es suficiente con informar en la web, si no que el cliente debería confirmar que ha leído y aceptado la política de privacidad

Que el consentimiento **explicito**

La ley establece que para determinado tipo de datos únicamente es válido el consentimiento explícito.

Para estos datos únicamente el consentimiento explícito puede considerarse válido, por tanto el consentimiento para cumplimentar los cuestionarios de salud, será siempre un consentimiento expreso de los datos.

El artículo 6 del reglamento europeo establece que para que el consentimiento sea lícito, es necesario que se cumpla cualquiera de los siguientes requisitos:

- **Que exista el consentimiento del interesado para el fin específico**. Es decir, que un fin adicional de tratamiento, como ocurre por ejemplo en la elaboración de perfiles a efectos de elaborar ofertas personalizadas para el afectado, requerirían un consentimiento adicional como una marcación de casilla extra.
- **Que el tratamiento sea necesario para la ejecución de un contrato** en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. Como por ejemplo: “La base legal para el tratamiento de sus datos es la ejecución del contrato de suscripción a las revistas que figuran en su cartera de pedidos (…según los términos y condiciones que constan en…)”, según establece la Agencia Española de Protección de Datos (en adelante la AEPD) en la guía del deber de información.
- **Que el tratamiento sea necesario para el cumplimiento de una obligación legal** aplicable al responsable del tratamiento.

- **Que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física**. En caso de estar una persona inconsciente y precisarse su información médica y ser una cuestión vital, dicha información podría proporcionarse sin que mediase el consentimiento del interesado
- Que el tratamiento sea necesario para el **cumplimiento de una misión realizada en interés público** o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- Que el tratamiento sea necesario para la **satisfacción de intereses legítimos** perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Un ejemplo sería los datos a aportar como pruebas a un juicio siempre que hayan sido obtenidos de forma lícita.

Requisitos del consentimiento

Los requisitos para que un consentimiento sea considerado válido son:

- **Información específica**: El consentimiento debe ser específico y basado en información adecuada. No es aceptable el consentimiento genérico sin especificar el propósito exacto de su finalidad.
- **Momento**: El consentimiento debe darse antes de que comience el tratamiento.
- **Elección activa**: El consentimiento debe ser inequívoco. Debe ser una indicación activa de la voluntad del interesado y no debe dejar ninguna duda en cuanto a su intención.
- **Libremente otorgado**: El consentimiento sólo será válido si el interesado está en condiciones de ejercer una elección real y no hay riesgo de engaño, intimidación, coacción o consecuencias negativas importantes si el interesado no da su consentimiento.

Condiciones del consentimiento

Las condiciones para que un consentimiento sea considerado válido son:

- El Responsable del tratamiento asumirá la **prueba del consentimiento**. Si éste se realiza por escrito, deberá distinguirse claramente de otros asuntos.
- El consentimiento no será lícito si se condiciona a una prestación de servicios sin ser necesario para su realización.
- El Responsable del tratamiento informará al interesado, antes de dar su consentimiento, que tiene derecho a retirarlo en cualquier momento sin que afecte al tratamiento efectuado hasta entonces.
- Debe ser tan fácil retirar como dar el consentimiento.
- Los consentimientos que infrinjan parcialmente el Reglamento serán considerados nulos.

Licitud del tratamiento

El tratamiento sólo será lícito cuando exista:

- El consentimiento explícito para fines específicos.
- Un contrato o precontrato con el interesado.
- La necesidad de la protección de los intereses vitales del interesado u otra persona física.
- Un interés legítimo del Responsable del tratamiento o de terceros, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, especialmente si es un niño.
- Una procedencia legítima de archivos de acceso público obtenidos de una fuente pública o el interesado haya hecho manifiestamente públicos sus datos. Un registro público sería la información de cargos de un profesional obtenidos del registro mercantil.
- Una obligación jurídica a la que esté sujeto el Responsable del tratamiento.
- Un cometido de interés público fundamentado en la legislación vigente.

Características del consentimiento

- La información a los interesados, tanto respecto a las condiciones de los tratamientos que les afecten como en las respuestas a los ejercicios de derechos, deberá proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo

- Se deberán evitar las fórmulas especialmente farragosas y que incorporan remisiones a los textos legales.
- Las clausulas informativas deberán explicar el contenido al que inmediatamente se refieren de forma clara y accesible para los interesados, con independencia de sus conocimientos en la materia.
- Se establece una lista exhaustiva de la información que debe proporcionarse a los interesados
    - Identidad y datos de contacto del Responsable del fichero
    - Finalidad(es) del tratamiento
    - Ejercicio de los derechos
    - Base jurídica del tratamiento
    - Intención de realizar transferencias internacionales
    - Datos del Delegado de Protección de Datos (si lo hubiere)
    - Elaboración de perfiles
- La información a los interesados deberá facilitarse por escrito, incluidos los medios electrónicos cuando sea apropiado.

<u>El consentimiento en menores</u>

En el artículo 8 del Reglamento Europeo se establecen las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.

- En relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.
- El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

Este tratamiento en menores obliga a las empresas a obtener el consentimiento de quien ostente la patria potestad del menor para conservar los datos de los menores, esto adquiere especial importancia en la gestión de datos en redes sociales, en las que un menor no podrá, si es menor de 16 años, acceder y proporcionar datos si no se ha recabado el consentimiento de los padres.

Siempre que tratemos con datos de menores de 16 años (colegios, seguros en los que haya relaciones de menores, actividades deportivas con menores, etc)

¿Cómo puede el empresario probar el consentimiento del titular de los datos?

La prueba del consentimiento del afectado en las empresas, vendrá determinado **por la firma del titular de los datos del documento en el que se le informa de la existencia del fichero**, así como de sus derechos de acceso, cancelación y rectificación y restante información requerida por la legislación vigente,

L firma por parte del mismo de un contrato en el que se incorpore la información de protección de datos, serían prueba de la existencia del ficheros, en caso de requerir la información previa formalización de un contrato para la realización de un presupuesto, debería existir un documento de consentimiento previo.

En caso en que entre el contrato y el presupuesto existiesen condicionantes diferentes del consentimiento (como pudiera ser el plazo de conservación de la información) se deberá presentar un nuevo documento de consentimiento.

El consentimiento deberá otorgarse para cada una de las finalidades, por lo que en caso de existir más de una finalidad, el interesado deberá poder seleccionar los consentimientos que otorga, por lo que en formularios de consentimiento en los que existan diferentes finalidades, deberá permitirse mediante casillas a cuales de las finalidades otorga el consentimiento.

Como deberíamos actuar en la captación de datos de los consentimientos en función de la forma en que contactemos con los mismos

- En la **visita personal del cliente**, la manera más adecuada sería **hacer firmar al cliente un documento** en el que le informamos de la existencia del fichero y su

finalidad, así como de la posibilidad de ejercer sus derechos. La firma del documento sería la prueba del consentimiento del afectado.

- En las **comunicaciones telefónicas**, debería proporcionarse, durante la conversación con el cliente y antes de informar sus datos en el fichero, de la existencia del fichero y su finalidad, así como de la posibilidad de ejercer sus derechos de acceso, rectificación y cancelación. **La forma de prueba sería la grabación de las conversaciones**, situación está de la que debería avisarse al cliente.

  En caso de no grabarse la conversación, debería complementarse la información proporcionada telefónicamente con el envío al cliente de la información de la existencia del fichero, finalidades y responsable frente al que se pueden ejercer los derechos de acceso, rectificación y cancelación, información que el cliente debería devolver firmada

- En el caso de captación por página web estaríamos a lo indicado anteriormente para el consentimiento implícito.

2. La calidad de los datos

La aplicación de este principio supone que los datos de carácter personal sólo podrán recogerse para su tratamiento cuando sean **adecuados, pertinentes** y **no excesivos** para el cumplimiento de las finalidades del fichero.

La normativa, a través del establecimiento de este principio, trata de introducir un criterio de racionalidad y proporcionalidad en el tratamiento de los datos personales.

Son varios los aspectos que deben tenerse en cuenta en relación a la calidad de los datos

Los datos recogidos deben ser acordes con la finalidad perseguida por el fichero

El principio de calidad de los datos, que, ligado al principio de proporcionalidad de los datos, exige que los mismos sean adecuados a la finalidad que motiva su recogida.

Antes de empezar a recoger los datos de carácter personal se deberá analizar la finalidad que se persigue con el fichero, ya que la Ley sólo legitima el uso de aquellos

que sean efectivamente necesarios por ser adecuados, pertinentes y no excesivos. En el pasado las empresas recogían datos con la finalidad de ampliar el perfil de sus clientes, siendo los datos muy superiores a los requeridos al encargo proporcionado por el cliente, esta práctica queda limitada por el principio de Calidad de los datos, debiendo el responsable del fichero limitar la recogida de los datos a los necesarios a la finalidad del fichero.

Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados

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

Otro de los efectos derivados del principio de la calidad de los datos, es que los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Los datos deben ser veraces

La creación de grandes bancos de datos personales de finalidad múltiple se ve limitada, adicionalmente, por la naturaleza variable de tales datos. La calidad de los datos nos exige igualmente que los datos sean ciertos, por lo que según qué datos de carácter variable, como el estado de salud, la edad o el sexo, se convierten en datos que han de ser justificados en su necesidad, cuando los mismos forman parte del fichero.

No puede olvidarse que según el principio de la calidad de los datos Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados.

Recogida de los datos

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

La recogida y tratamiento de datos de carácter personal debe efectuarse desde su subordinación a los principios de calidad de los datos y de proporcionalidad que establece la Ley.

Sentencias en relación a la calidad de los datos

El Tribunal Constitucional en la Sentencia 292/2000, de 30 de noviembre, amplia el principio a lo que denomina derecho de autodeterminación informativa o de libre disponibilidad de los datos de carácter personal.

Dicha sentencia determina que este derecho fundamental 'persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado', estableciendo, en cuanto a su ámbito, que 'el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18. 1 CE otorga, sino los datos de carácter personal'.

En relación al control sobre los datos personales la mencionada sentencia establece: 'se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos'.

3. Los llamados datos sensibles o categorías especiales de datos

Los datos sensibles establecidos en la legislación española, son igualmente reflejados en el artículo 9 del reglamento europeo de protección de datos

Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física"

Nadie podrá ser obligado a declarar sobre su ideología, religión, afiliación sindical o creencias, y sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento. Los datos relativos a la salud, en caso de ser tratados en relaciones comerciales a través de Internet, sólo pueden serlo por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto, y siempre bajo el consentimiento expreso e informado del usuario.

No podríamos contemplar en nuestras páginas web la recogida de datos sensibles y de hacerlo debería existir una justificación y base legal para su captación y deberíamos restringir el acceso a esta información a personal especializado con la obligación de secreto profesional, adicionalmente sería exigible un servidor seguro.

4. La cesión/ Transmisión de datos

La transmisión o cesión de datos viene regulada tanto por la normativa europea como por la ley orgánica

En cuanto a la cesión de datos, si la misma comporta identificación de concretas personas físicas constituye una comunicación de datos de carácter personal, definida en el artículo 3, i) de la Ley Orgánica 15/1999, como "toda revelación de datos realizada a persona distinta del interesado".

El régimen de las cesiones de datos se contiene en el artículo 11 de la citada Ley Orgánica:

Artículo 11. Comunicación de datos.

"Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las

funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

El consentimiento exigido en el apartado anterior no será preciso:

- Cuando la cesión está autorizada en una Ley.
- Cuando se trate de datos recogidos de fuentes accesibles al público.
- Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. Un ejemplo sería la información que una autoescuela proporcione a tráfico para la realización del examen de conducir de un alumno.
- Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso 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 cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.

El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

Aquél a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la normativa de protección de datos.

Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores."

En cuanto al reglamento 2016/679 del parlamento europeo establece la posibilidad de realizar transferencias en determinadas circunstancias:

- Con el consentimiento explícito del interesado,
- Si la transferencia es ocasional y necesaria en relación con un contrato o una reclamación, independientemente de tratarse de un procedimiento judicial o un procedimiento administrativo o extrajudicial, incluidos los procedimientos ante organismos reguladores.
- Cuando así lo requieran razones importantes de interés público establecidas por el Derecho de la Unión o de los Estados miembros.
- Cuando la transferencia se haga a partir de un registro establecido por ley y se destine a consulta por el público o por personas que tengan un interés legítimo, permitiéndose únicamente la transmisión de las categorías de datos incluidos en el registro. Si el registro está destinado a la consulta por personas que tengan un interés legítimo, la transferencia solo debe efectuarse a petición de dichas personas o, si estas van a ser las destinatarias, teniendo plenamente en cuenta los intereses y los derechos fundamentales del interesado. Ejemplo de esta casuística es el Registro de Contratos de Seguros de cobertura de fallecimiento
- Las transferencias de datos requeridas y necesarias por razones importantes de interés público, por ejemplo en caso de intercambios internacionales de datos entre autoridades en el ámbito de la competencia, administraciones fiscales o aduaneras, entre autoridades de supervisión financiera, entre servicios competentes en materia de seguridad social o de sanidad pública, por ejemplo las notificaciones a la agencia tributaria o a la seguridad social.

- En caso de que sea necesaria para proteger un interés esencial para los intereses vitales del interesado o de otra persona, incluida la integridad física o la vida, si el interesado no está en condiciones de dar su consentimiento.

Hemos visto en que supuestos está permitida la cesión o transmisión de datos, pero que entendemos por el mismo.

Cesión o comunicación de datos sería por tanto la revelación a cualquier persona que no sea el propio interesado.

En esta definición debemos entender que incluso la comunicación a familiares del interesado tienen la consideración de cesión de datos a terceros.

Como principio general, la cesión o comunicación de datos requiere el consentimiento del afectado, por lo que para proporcionar información a familiares, requeriremos el consentimiento inequívoco y expreso del afectado.

En la práctica ello supone que si el interesado o titular de los datos desea que algún familiar acceda a su información o bien pueda recoger su documentación, debe estar previamente autorizado, lo que obliga al responsable del fichero a mantener la información de las personas autorizadas, autorización que deberá proporcionarse identificando a las personas autorizadas con nombre, apellidos y DNI.

La cesión de datos especialmente protegidos que revelen la ideología, religión, creencias, origen racial o vida sexual sólo podrán ser comunicados con el consentimiento expreso del afectado.

5. El encargado del tratamiento

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

El encargado de tratamiento está legitimado para acceder a los datos personales obrantes en el fichero sin el requisito del consentimiento previo del afectado, siempre que la relación entre el primero y el responsable del fichero esté formalizada en un contrato que obedezca a fines lícitos y legítimos y se especifiquen las condiciones en

que se va a llevar a cabo el tratamiento y que la utilización de los datos será únicamente para los fines establecidos por el responsable del fichero.

Un ejemplo típico de encargado del tratamiento es la empresa con la que podemos establecer una relación contractual para que se encargue de la destrucción de los documentos que contienen datos de carácter personal y ya no tengo por qué mantener en mis archivos o el asesor laboral o fiscal de la empresa

La normativa vigente establece que responsable del tratamiento debe elegir un encargado de tratamiento con garantías suficientes de cumplimiento, incluye la necesidad de supervisar de manera periódica, por ejemplo mediante auditorias, que el encargado del tratamiento tiene implementadas las medidas de seguridad adecuadas sobre los datos de carácter personal.

LA adhesión a códigos de conducta o acreditar la posesión de un certificado en materia de protección de datos se consideran factores en la obtención de garantías suficientes en la elección del encargado del tratamiento por parte del responsable.

La relación entre el responsable y el encargado del tratamiento, ésta deberá establecerse a través de un contrato o de un acto jurídico similar que los vincule. El contrato o acto jurídico deberá constar por escrito, inclusive en formato electrónico. En particular, el acuerdo o acto que se suscriba entre el responsable y el encargado del tratamiento deberá contener como mínimo las siguientes obligaciones y responsabilidades:

- Tipo de datos personales y categorías de interesados
- Obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable. inclusive en relación a las transferencias de datos personales a un tercer país o una organización internacional.
- Condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones

  Cuando un encargado quiera recurrir a otro para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, será necesaria la autorización previa por escrito, específica o general del responsable. En caso de aprobarse la subcontratación, el encargado se impondrá a este otro

mediante un contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros.

- Asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados.
- Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.
- Que adoptará las medidas de seguridad necesarias, conforme a lo dispuesto en la normativa vigente de protección de datos. El encargado del tratamiento deberá aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
- El encargado deberá facilitar al responsable, la información necesaria para demostrar el cumplimiento de todas sus obligaciones en materia de protección de datos, incluyendo la realización de auditorías o inspecciones. De igual manera, éste informará de manera inmediata al responsable si, en su opinión, una instrucción infringe el Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los estados miembros.
- Finalizado el tratamiento, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que se requiera la conservación de dichos datos en virtud de la normativa vigente.

Ejemplos de encargados de tratamiento con los que deberemos establecer el contrato de tratamiento de datos por cuenta de terceros serán: el asesor fiscal y/o laboral, el responsable del mantenimiento informático si es externo a la empresa o empresas con las que se tengan subcontratados servicios de atención telefónica.

Los encargados tienen obligaciones propias que establece la legislación vigente, que no se circunscriben al ámbito del contrato que los une al responsable, y que pueden ser supervisadas separadamente por las autoridades de protección de datos, entre otras:

- Deben mantener un registro de actividades de tratamiento.
- Deben determinar las medidas de seguridad aplicables a los tratamientos que realizan.

- Deben designar a un Delegado de Protección de Datos en los casos previstos por la legislación vigente

Elección del encargado de tratamiento

Los responsables habrán de elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento. Esta previsión se extiende también a los encargados cuando subcontraten operaciones de tratamiento con otros subencargados.

Para dar cumplimiento a esta exigencia los responsables de tratamiento deberán desarrollar modelos de evaluación de los proveedores que les permitan certificarles en el cumplimiento de los preceptos de protección de datos.

Esta evaluación deberá realizarse con todo proveedor que vaya a tratar datos personales con independencia de la naturaleza de los mismos, tanto si son datos de los trabajadores, como de los clientes y de cualquier otro colectivo existente en los ficheros de la empresa

MEDIDAS DE RESPONSABILIDAD ACTIVA

Análisis del riesgo

Las empresas y profesionales deben adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece. El Reglamento entiende que actuar sólo cuando ya se ha producido una infracción es insuficiente como estrategia, dado que esa infracción puede causar daños a los interesados que pueden ser muy difíciles de compensar o reparar a posteriori.

El primer paso para determinar qué medidas deben adoptarse es la realización de un Análisis sobre los Riesgos que los tratamientos de datos que estamos haciendo o hemos planificado puedan significar para los derechos y libertades de los interesados.

El legislación vigente condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados-. Se maneja el riesgo de dos maneras:

- En algunos casos, prevé que determinadas medidas solo deberán aplicarse cuando el tratamiento suponga un alto riesgo para los derechos y libertados (por ejemplo, Evaluaciones de impacto sobre la Protección de Datos).
- En otros casos, las medidas deberán modularse en función del nivel y tipo de riesgo que el tratamiento conlleve (por ejemplo, con las medidas de Protección de Datos desde el Diseño o con las medidas de seguridad).

Todos los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo. Las medidas a adoptar dependerán de:

- Los riesgos inherentes al tratamiento y la probabilidad de causar perjuicios a los derechos y libertades de las personas físicas.
- La naturaleza, contexto, ámbito y fines del tratamiento.
- La duración en el tiempo del tratamiento de dichos datos y su conservación.
- El estado de la técnica.
- El coste de la aplicación de las medidas.
- La cantidad de datos personales recogidos.
- Grado de accesibilidad de los datos.

Dos son los conceptos a tener presente en el proceso de análisis del riesgo y son la protección de datos desde el diseño y la protección de datos por defecto. Ambos conceptos, tienen como premisa, garantizar los derechos y libertades de los interesados desde la definición de una actividad de tratamiento. El responsable del tratamiento que realiza o desea realizar actividades de tratamiento con datos

personales, debe establecer procedimientos de control que garanticen cumplir los principios de protección desde el diseño y por defecto.

Protección de datos desde el diseño:

Ante la constante evolución tecnológica y los procesos de transformación digital que sufren las actividades de tratamiento de datos personales, la regulación de protección de datos establece un modelo enfocado en la gestión continua de los riesgos potenciales asociados al tratamiento desde su diseño.

El diseño adecuado de las actividades de tratamiento es un aspecto clave para poder garantizar los derechos y libertades de los interesados. La fase de diseño de un tratamiento define el flujo de los datos personales, así como todos los elementos que intervendrán a lo largo del mismo.

De igual modo, es el momento idóneo para definir las medidas de control y seguridad para garantizar los derechos y libertades de los interesados con el objetivo de que un tratamiento nazca respetando los requerimientos de privacidad asociados al nivel de riesgo a la que está expuesto.

La protección de datos desde el diseño consiste en la implantación de medidas y procesos que permitan acreditar el cumplimiento de la normativa en materia de protección de datos desde el mismo momento de la concepción de un nuevo producto o servicio.

Esta medida resulta útil no sólo por el cumplimiento normativo, sino por permitirnos identificar, corregir o mitigar posibles problemas desde una fase muy temprana, y por lo tanto, con el menor coste posible.

Protección de datos por defecto:

Consiste en garantizar por defecto que únicamente sean objeto de tratamiento los datos personales necesarios para el cumplimiento de las finalidades previstas y que éstos sean únicamente accesibles por el número de personas indispensable para llevar a cabo la acción deseada.

Definición y diseño de las actividades de tratamiento

La definición de una actividad de tratamiento tiene por objeto en la empresa saber cuáles son las finalidades del tratamiento de datos personales.

Una vez establecido el registro de tratamientos de la entidad en el que se reflejarán todas aquellas actividades que corresponden al trabajo o funciones que esta realiza sobre los datos de carácter personal de los colectivos de personas que maneja, deberá realizarse la evaluación de riesgo y valorarse cada uno de los mismos

Se establecen los siguientes principios relativos al tratamiento de datos personales que es necesario considerar en la definición de un tratamiento:

- **Licitud, lealtad y transparencia**: Los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado.

- **Limitación de la finalidad**: Los datos se deben recoger con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
- **Minimización de datos**: Los datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- **Exactitud:** Los datos deben ser exactos, y si fuera necesario, actualizados. Además, se establece que se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación si los datos son inexactos con respecto a los finales para los que se tratan.
- **Limitación del plazo de conservación**: Los datos deben ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.
- **Integridad y confidencialidad:** Los datos deben ser tratados de tal manera que se garantice una seguridad adecuada mediante la aplicación de medidas de control apropiadas.

Evaluar la necesidad de realizar un EIPD

Para cada una de las actividades evaluaremos en primer lugar de necesidad de realizar o no una Evaluación de impacto sobre la protección de datos (EIPD)

Un análisis previo nos permitirá establecer para cada actividad de tratamiento la necesidad o no, los criterios vienen marcados por

1. Listas de tratamientos **previstos en la legislación**, en la que se establecen tres casos en los que es obligatorio

    - Tratamientos evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

    - Tratamiento a gran escala de las categorías especiales de o de los datos personales relativos a condenas e infracciones penales

    - Tratamientos que comporte la observación sistemática a gran escala de una zona de acceso público.

2. La naturaleza, alcance, contexto y fines de tratamiento

    Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnología, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para las libertades y derechos deberá realizarse la EIPD

    Naturaleza del tratamiento: Hemos de tener en consideración si se trata o no de categorías especiales de datos, si el tratamiento es o no a gran escala, si se realiza un seguimiento exhaustivo de las personas, etc.... Las naturalezas de tratamiento que se correspondan con grupos especialmente

vulnerables como grupos con dependencia nos llevarán a realizar un EIDP, igualmente los datos de menores, estos son ejemplos, pero ha de ser cada empresa quien evalúe si en función de la naturaleza es preciso.

Alcance del tratamiento: Hemos de valorar las consecuencias del tratamiento, identificando el riesgo que comporta para los titulares de los datos, por ejemplo si puede tener consecuencias jurídicas, si se valora el riesgo crediticio, tratamientos que determinen la otorgación de subsidios. Si existen riesgos importantes para el interesado nos veremos obligados a realizar un EIPD

Contexto del tratamiento: Se debe valorar el conjunto de circunstancias bajo las cuales se realizarán las actividades de tratamiento, con el objetivo de verificar si pueden suponer un alto riesgo. Son factores que incrementan el riesgo son:

- Se usan nuevas tecnologías especialmente invasivas para la privacidad (tratamientos como Facebook u otras redes sociales
- Hay varios responsables del tratamiento
- Hay más de un encargado del tratamiento
- Se producen transferencias internaciones de datos
- Se producen cesiones de datos

Finalidades del tratamiento; deben evaluarse cada una de las finalidades y analizar si comportan o no un elevado riesgo, como sería el caso de

- Toma de decisiones automatizadas
- Elaboración de perfiles
- Análisis predictivo
- Prestación de servicios relativos a la Salud
- Monitorización de personas

Como resultado del análisis de los elementos anteriores determinaremos la necesidad o no de realizar una EIPD:

- **Sí es necesario realizar una EIPD**: Se realizará y documentará una EIPD con todas sus fases
- **No es necesario realizar una EIPD:** Se entiende que las actividades de tratamiento no están expuestas a riesgos relevantes que motiven la necesidad de realizar una EIPD en profundidad.
  Si como resultado del análisis previo se considera que no es necesario llevar a cabo una EIPD, se debe documentar adecuadamente los motivos por los cuales se ha llegado a esa conclusión. En cualquier caso, se debe mantener evidencia de que se ha llevado a cabo este análisis (responsabilidad proactiva).

Registro de actividades de tratamiento

La normativa vigente de protección de datos establece:

"Cada responsable y, en su caso, su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad". Adicionalmente indica que "cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable".

Es importante identificar en que consiste un tratamiento, que se define como el conjunto de operaciones dirigidas a conseguir una determinada finalidad que se legitiman en una misma base jurídica. Cada tratamiento incluirá una serie de operaciones como, por ejemplo la recogida, registro, organización, estructuración, consulta o utilización de los datos.

En base a esta definición no definiremos como tratamientos Gestión de RRHH y gestión de nóminas, sino que podremos establecer que el tratamiento es gestión laboral ya que ambos tratamientos tienen una única finalidad cual es gestionar los RRHH de la empresa.

Una actividad de tratamiento se debe incluir en el registro de actividades en el momento previo antes de su puesta en marcha. Para facilitar la documentación del registro se puede utilizar la información previa documentada en los análisis iniciales realizados durante la fase de definición de la operación de tratamiento.

Cada responsable de tratamiento deberá valorar el grado de segregación o agregación al que somete sus tratamientos generando elementos diferentes que se corresponden con finalidades, bases jurídicas y grupos de individuos distintos.

Para cada tratamiento existente en el registro debe hacerse la evaluación previa y si corresponde el EIPD

El registro de actividades del responsable del fichero deberá contener al menos

- el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
- los fines del tratamiento;
- una descripción de las categorías de interesados y de las categorías de datos
- personales;
- las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las trasferencias internacionales a

países no asimilados en protección de datos, se incluirá, la documentación de garantías adecuadas;
- cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
- cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad adoptadas.

En el caso de encargados de tratamiento, el registro de actividades deberá contener al menos

- el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
- las categorías de tratamientos efectuados por cuenta de cada responsable; en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional
- y, en el caso de las transferencias internacionales a países no asimilados en materia de protección de datos, la documentación de garantías adecuadas;
- cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad

Análisis básico de los riesgos

Las actividades de tratamiento que no requieren una EIPD, requieren el análisis de riesgos para determinar las medidas técnicas y organizativas que garanticen los derechos y libertades de los interesados se puede simplificar con un enfoque de mínimos considerando que el nivel de riesgo al que están expuestas las actividades de tratamiento no es elevado.

El análisis básico de riesgos es un análisis de mínimos que tiene como objetivo simplificar el proceso de análisis de riesgos en aquellas actividades de tratamiento con baja exposición al riesgo.

Como punto de partida, de igual modo que en una EIPD, se deben describir adecuadamente las actividades de tratamiento, proceso que facilitará la documentación del registro de actividades de tratamiento.

A partir del registro de actividades se realizarán varios pasos

Descripción de las operaciones de actividades de tratamiento

La descripción de los tratamientos sujetos al análisis de riesgos, permite obtener un conocimiento del ciclo de vida de los datos, de las actividades realizadas y de cualquier elemento que interviene en las mismas.

En este análisis agruparemos las actividades de tratamiento por procesos comunes expuestos a riesgos similares

El ciclo de vida de los datos se puede dividir en las siguientes etapas:

Captura de datos: Proceso de obtención de datos para su almacenamiento y posterior procesado. La captura de datos se puede realizar por diferentes medios: formularios web, formularios en papel, toma de muestras y realización de encuestas, grabaciones de audio y video, redes sociales, etc.

Clasificación / Almacenamiento: Establecer categorías y asignarlas a los datos para su clasificación y almacenamiento en los sistemas o archivos.

Uso / Tratamiento: Operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos de los datos automatizados o manuales.

Cesión o transferencia de los datos a un tercero para su tratamiento: Traspaso o comunicación de datos realizada a un tercero, definido como aquella persona física o jurídica, pública o privada u órgano administrativo. Este concepto es muy amplio, puesto que recoge tanto la entrega, comunicación, consulta, interconexión, transferencia, difusión o cualquier otra forma de acceso a los datos.

Destrucción: Eliminar los datos que puedan estar contenidos en los sistemas o archivos, de manera que no puedan ser recuperados de los soportes de almacenamiento

Actividades de tratamiento sobre los datos de carácter personal

Una actividad de tratamiento responde a la materialización de una finalidad sobre los datos personales de un determinado colectivo de personas. Así una actividad de tratamiento puede ser la gestión de personal, la gestión fiscal, la gestión de alumnos, la gestión de un servicio, la gestión de los seguros.

En este paso, se deben considerar todas las actividades u operaciones de tratamiento similares y que están expuestas a los mismos riesgos, con el objetivo de establecer medidas de control comunes que permitan reducir su nivel de exposición. El enfoque de análisis de riesgos global, busca la agrupación de procesos, actividad que simplifica el análisis sin reducir su nivel de temas similares o bases de datos con una tipología concreta.

También puede ser criterio de la organización agrupar las actividades de tratamiento entre aquellas que atiendan a finalidades similares sobre grupos de individuos diferentes un ejemplo sería la contabilización de facturas de clientes y proveedores y su tratamiento a nivel fiscal, si bien son grupos diferentes, podemos realizar un análisis conjunto

Para cada actividad de tratamiento definiremos

- **Datos**

Estableceremos las tipologías de datos e interrelaciones entre los mismos, establecimiento el grado de importancia dentro de las actividades de tratamiento y si estamos ante un dato que es o no imprescindible para el tratamiento, asegurándonos de que no se recogen datos que no son necesarios para la actividad de tratamiento

- **Intervinientes**

  Identificaremos los intervinientes, las personas físicas o jurídicas que están implicadas en las actividades del tratamiento, definiendo sus funciones y responsabilidades.

  Dentro de este grupo se puede incluir el responsable del tratamiento, áreas o empleados de las organizaciones que participan activamente del procesado de los datos, encargados de tratamiento, etc.

  La participación de cada uno de los intervienes puede suponer una amenaza sobre los datos de carácter personal, debiendo establecerse las medidas tendentes a minimizar el riesgo.

- **Tecnología**

  La tecnología y los sistemas de información en un elemento clave que da soporte a las actividades de tratamiento de los datos de carácter personal. Se debe identificar aquellos elementos tecnológicos implicados (tanto hardware como software) en las actividades de tratamiento

  Para actividades de tratamiento con soporte en la misma tecnología, la exposición a los riesgos derivados de su uso será similar y, por tanto, se podrá agrupar bajo este criterio las actividades de tratamiento a la hora de identificar, evaluar y tratar los mismos.

  Por último, no hay que olvidar que, si alguna actividad de tratamiento implica el procesamiento no automatizado de los datos, se ha de identificar como una actividad más de tratamiento e inventariar como un activo más.

Gestión de los riesgos

Para cada una de las actividades de riesgo se establecerá la probabilidad del riesgo situándolos en dos niveles

- **Riesgos asociados a la protección de la información** con foco en la integridad, disponibilidad y confidencialidad de los datos. Por ejemplo, acceso ilegítimo a los datos o pérdida de datos.
- **Riesgos asociados al cumplimiento de los requisitos regulatorios** relacionados con los derechos y libertades de los interesados. Por ejemplo, uso ilegítimo de datos personales o la posibilidad de que el responsable no pueda atender el ejercicio de los derechos establecidos por la legislación vigente

En cada actividad de tratamiento, se debe analizar y determinar cuáles de los riesgos situados dentro de las dimensiones de protección de los datos personales y derechos y libertades de los interesados son de aplicación. A continuación, para cada uno de los riesgos identificados, se deberán establecer tantas medidas de seguridad como sean necesarias para garantizar un nivel de seguridad y control adecuado que reduzca la exposición al riesgo.

Para cada riesgo identificado estableceremos las medidas de control del riesgo tendentes a eliminar o aminorar la probabilidad de que se produzca un efecto no deseado en el tratamiento de los datos

Ejemplo

Tipología de Riesgo	Riesgo	Medidas de control
Integridad de los datos personales	Modificación o alteración de datos personales no intencionada	• Segregación de funciones mediante perfiles de acceso • Controles de monitorización de amenazasen red
Disponibilidad de los datos personales	Pérdida o borrado no intencionado de datos personales	• Copias de seguridad • Almacenamiento en dos ubicaciones diferentes

Los riesgos identificados y las medidas de control definidas deben documentarse, con el objetivo de evidenciar la evaluación de riesgos realizada y tener una base de trabajo ante futuras revisiones del análisis derivadas de cambios en las actividades de tratamiento.

Los riesgos son variables y pueden cambiar ante variaciones en las actividades de tratamiento. Garantizar una adecuada gestión de riesgos requiere la monitorización continua de los riesgos y la evaluación periódica de la efectividad de las medidas de control definidas para reducir el nivel de exposición al riesgo.

Notificación de “violaciones de seguridad de los datos

las violaciones de seguridad de los datos, más comúnmente conocidas como “brechas de seguridad”, han de ser entendidas de una forma muy amplia, que abarca todo percance que originen la destrucción, pérdida o modificación accidental o ilícita de datos personales cedidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Incidentes como la pérdida de un expediente en papel, el cifrado de las bases de datos por efecto de un virus o el borrado accidental de algunos registros son consideradas violaciones de seguridad y se ha de actuar en estos casos conforme establece la legislación vigente

Las obligaciones que surgen en caso de violaciones de seguridad son

- Notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados. La notificación a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.
- La notificación ha de incluir un contenido mínimo:
    - la naturaleza de la violación
    - categorías de datos y de interesados afectados
    - medidas adoptadas por el responsable para solventar la quiebra
    - si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados
- Los responsables deben documentar todas las violaciones de seguridad.
- En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con una notificación dirigida a estos últimos

  El objetivo de la notificación a los afectados es permitir que puedan tomar medidas para protegerse de sus consecuencias. Por ello, la legislación vigente requiere que se realice sin dilación indebida, sin hacer referencia ni al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas. El propósito es siempre que el interesado afectado pueda reaccionar tan pronto como sea posible.

  La notificación a los interesados no será necesaria cuando:
    - El responsable hubiera tomado medidas técnicas u organizativas apropiadas con anterioridad a la violación de seguridad, en particular las medidas que hagan ininteligibles los datos para terceros, como sería el cifrado.
    - Cuando el responsable haya tomado con posterioridad a la quiebra medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice.
    - Cuando la notificación suponga un esfuerzo desproporcionado, debiendo en estos casos sustituirse por medidas alternativas como puede ser una comunicación pública.
- Las recomendaciones sobre las medidas que pueden tomar los interesados para hacer frente a las consecuencias de la quiebra

Valoración del riesgo

La **valoración del riesgo** de la quiebra es diferente del análisis de riesgos previo a todo tratamiento. Cuando se produce la quiebra de seguridad lo que se pretende determinar hasta qué punto el incidente, por sus características, el tipo de datos a los que se refiere o el tipo de consecuencias que puede ocasionar a los afectados puede causar un daño en los derechos o libertades de los afectados.

Tipo de daños

Los **daños pueden ser materiales o inmateriales**, e ir desde la posible discriminación de los afectados debido al uso de sus datos personales por quien ha accedido a ellos de forma no autorizada hasta la suplantación de identidad, pasando por daños económicos o la exposición pública de datos confidenciales.

En qué momento

Se entiende que se tiene conocimiento de una violación de seguridad cuando hay una **certeza de que se ha producido** y se tiene un conocimiento suficiente de su naturaleza y alcance.

La mera sospecha de que se ha producido una quiebra o la constatación de que ha sucedido algún tipo de incidente sin que se conozcan mínimamente sus circunstancias no deberían dar lugar, todavía, a la notificación, dado que en esas condiciones no sería posible, en la mayoría de los casos, evaluar hasta qué punto puede originarse un riesgo para los derechos y libertades de los interesados.

Nivel de impacto

En supuestos de quiebras que por sus características pudieran tener gran impacto, sí sería aconsejable ponerse en contacto con la autoridad de supervisión tan pronto como **existan indicios** de que se ha producido alguna situación irregular respecto a la seguridad de los datos. Sin perjuicio de que esos primeros contactos puedan completarse con una notificación formal más completa dentro del plazo legalmente previsto.

Otras consideraciones

Puede haber casos en que la notificación no pueda realizarse dentro de esas 72 horas, por ejemplo, por la complejidad en determinar completamente su alcance. En esos casos, es posible hacer la notificación con posterioridad, acompañándola de una explicación de los motivos que han ocasionado el retraso.

La información puede proporcionarse de forma escalonada cuando no sea posible hacerlo en el mismo momento de la notificación.

Evaluación de Impacto sobre la Protección de Datos

Los responsables de tratamiento deberán realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados.

Una PIA o una Evaluación de Impacto en la Protección de los Datos Personales (EIPD) es, en esencia, un ejercicio de análisis de los riesgos que un determinado sistema de información, producto o servicio puede entrañar para el derecho fundamental a la protección de datos de los afectados y, tras ese análisis, afrontar la gestión eficaz de los riesgos identificados mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos.

La gran ventaja derivada de la realización de una EIPD en las etapas iniciales del diseño de un nuevo producto, servicio o sistema de información es que permite identificar los posibles riesgos y corregirlos anticipadamente, evitando los costes derivados de descubrirlos a posteriori, cuando el servicio está en funcionamiento o, lo que es peor, cuando la lesión de los derechos se ha producido. En estos casos no solo se incurre en costes económicos, sino también de imagen para la organización cuya reputación se ve afectada.

Características de una EIPD

- Una EIPD es un proceso más amplio que el de la mera comprobación del cumplimiento normativo, que debe llevarse a cabo con anterioridad a la implantación de un nuevo producto, servicio o sistema de información o cuando uno existente vaya a sufrir cambios sustanciales que impliquen la posibilidad de la aparición de nuevos riesgos.
- Debe ser sistemática y reproducible, y estar orientada a revisar procesos más que a producir un resultado o informe final. Además, debe permitir una identificación clara de los responsables de las distintas tareas.
- Comienza con una primera fase de identificación y clasificación de la información para determinar los datos personales que se tratan y sus características.
- Debe identificar quién y cómo tendrá acceso y tratará los datos personales.
- Se debe permitir participar en el proceso y realizar aportaciones a todos los afectados por el mismo, tanto departamentos de la organización como socios o entidades externas, afectados u otros agentes sociales.
- Debe contener una descripción de los controles que se implantarán para asegurar que solo se tratan los datos personales necesarios y para las finalidades legítimas previstas y definidas.
- El resultado final debe ser un documento con un contenido mínimo y una estructura que deben definirse previamente.
- Este resultado final de una EIPD debería tener un cierto grado de publicidad en un documento distribuido por la organización que la ha realizado y que, por supuesto, no contendrá información confidencial o sensible

Contenido mínimo

El contenido mínimo de las Evaluaciones de Impacto sobre la Protección de Datos

- Descripción del tratamiento y finalidades

  Se deberá llevar a cabo un análisis en profundidad del proyecto, obteniendo el detalle de las categorías de datos que se tratan, los usuarios de los mismos, los flujos de información y las tecnologías utilizadas.

- Evaluación de la proporcionalidad y necesidad del tratamiento

  Las autoridades de protección de datos a menudo señalan que para comprobar si una operación de tratamiento supone una medida restrictiva de un derecho

fundamental, esta operación tiene que superar los tres puntos del llamado juicio de proporcionalidad:

Juicio de idoneidad

Que la medida pueda conseguir el objetivo propuesto.

Juicio de necesidad

Si, además, es necesaria, en el sentido de que no existe otra más moderada para conseguir este propósito con la misma eficacia.

Juicio de proporcionalidad en sentido estricto

Si la medida es ponderada o equilibrada, porque se derivan más beneficios o ventajas para el interés general que no perjuicios sobre otros bienes o valores en conflicto.

Por lo tanto, la proporcionalidad tiene que ver con evaluar si la finalidad que se persigue se puede conseguir por otros medios, por ejemplo: usando otros datos (o menos datos), reduciendo el colectivo de personas afectadas (cuantitativamente o cualitativamente hablando), usando otras tecnologías menos invasivas o aplicando otros procedimientos o medios de tratamiento modificando los inicialmente previstos, etc.

- Evaluación de los riesgos

  Se tiene que llevar a cabo un análisis de los posibles riesgos para la protección de datos de los afectados y valoración de la probabilidad y el impacto de su materialización.

- Medidas previstas

  Una vez analizado los riesgos se deben establecer **medidas para afrontarlos.**

  Es decir se deben establecer garantías en función de los mismos mediante las cuales se garantice la protección de los datos personales, así como también que todos los procedimientos cumplen escrupulosamente con la normativa, siempre sin perder de vista los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Cuando el análisis de riesgo que las organizaciones lleven a cabo sobre los tratamientos indiquen que esos tratamientos presentan alto riesgo para los derechos o libertades de los interesados, con independencia de que dichos tratamientos ya sean operativos, los responsables deberán realizar una EIPD sobre esos tratamientos, a fin de estar en condiciones de poder adoptar las medidas adecuadas para adecuar esos tratamientos a las exigencias legislativas.

En los casos en que las EIPD hayan identificado un alto riesgo que, a juicio del responsable de tratamiento no pueda mitigarse por medios razonables en términos de tecnología disponible y costes de aplicación, el responsable deberá consultar a la

autoridad de protección de datos competente. La consulta debe ir acompañada de la documentación que prevé la legislación vigente, incluyendo la propia Evaluación de Impacto, y la autoridad de supervisión puede emitir recomendaciones o ejercer cualquier otro de los poderes que la legislación le confiere, entre ellos el de prohibir la operación de tratamiento.

Situaciones en las que sería aconsejable llevar a cabo una evaluación de impacto

- Cuando se enriquezca la información existente sobre las personas mediante la recogida de nuevas categorías de datos o se usen las existentes con nuevas finalidades o en formas que antes no se usaban, en particular, si los nuevos usos o finalidades son más intrusivos o inesperados para los afectados.
- Cuando se lleve a cabo un tratamiento significativo no incidental de datos de menores o dirigido especialmente a tratar datos de estos, en particular si tienen menos de catorce años.
- Cuando se vaya a llevar a cabo un tratamiento destinado a evaluar o predecir aspectos personales relevantes de los afectados, su comportamiento, su encuadramiento en perfiles determinados (para cualquier finalidad), encaminado a tomar medidas que produzcan efectos jurídicos que los atañen o los afectan significativamente y, en particular, cuando establezcan diferencias de trato o trato discriminatorio o que puedan afectar a su dignidad o su integridad personal
- Cuando se traten grandes volúmenes de datos personales a través de tecnologías como la de datos masivos (Big data), internet de las cosas (Internet of Things) o el desarrollo y la construcción de ciudades inteligentes (smart cities).
- Cuando se vayan a utilizar tecnologías que se consideran especialmente invasivas con la privacidad como la video vigilancia a gran escala, la utilización de aeronaves no tripuladas drones), la vigilancia electrónica, la minería de datos, la biometría, las técnicas genéticas, la geolocalización, o la utilización de etiquetas de radiofrecuencia o RFID (especialmente, si forman parte de la llamada internet de las cosas) o cualesquiera otras que puedan desarrollarse en el futuro.
- Cuando el tratamiento afecte a un número elevado de personas o, alternativa o adicionalmente, se produzca la acumulación de gran cantidad de datos respecto de los interesados.
- Cuando se cedan o comuniquen los datos personales a terceros y, en particular, siempre que se pongan en marcha nuevas iniciativas que supongan compartir datos personales con terceros que antes no tenían acceso a ellos, ya sea entregándolos, recibiéndolos o poniéndolos en común de cualquier forma.
- Cuando se vayan a transferir los datos a países que no forman parte del Espacio Económico Europeo (EEE) y que no hayan sido objeto de una declaración de adecuación por parte de la Comisión Europea o de la Agencia Española de Protección de Datos
- Cuando se vayan a utilizar formas de contactar con las personas afectadas que se podrían considerar especialmente intrusivas.
- Cuando se vayan a utilizar datos personales no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica.

- Cuando la recogida tenga como finalidad el tratamiento sistemático y masivo de datos especialmente protegidos

Delegado de Protección de Datos

Esta figura constituye uno de los elementos claves de la legislación de protección de datos y es un garante del cumplimiento de la normativa de protección de datos en las organizaciones y se encargará de asesorar e informar a las empresas sobre el grado de cumplimiento legislativo en materia de protección de datos

Funciones del delegado de protección de datos

- **Informar y asesorar** al responsable o al encargado de la empresa del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben y de otras disposiciones de protección de datos de la Unión Europea.
- **Supervisar el cumplimiento** de lo dispuesto en el Reglamento Europeo de Protección de Datos, así como de otras disposiciones entre las que se incluyen la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones en las que emplean datos personales.
- **Ofrecer el asesoramiento** que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con la normativa.
- **Cooperar con la autoridad de control** tanto europea como del país al que pertenezca en el ámbito de la privacidad de los datos personales.
- **Actuar como punto de contacto de la autoridad de control** para cuestiones relativas al tratamiento, incluida la consulta previa sobre cualquier otro asunto relacionado con la normativa.
- El delegado de protección de datos desempeñará sus funciones prestando la **debida atención a los riesgos asociados a las operaciones de tratamiento**, teniendo en cuenta la naturaleza, el alcance, el contexto de los datos empleados.

Quienes están obligados a nombrar un Delegado de protección de datos

- Autoridades y organismos públicos
- Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala
- Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles

Designación del delegado de protección de datos

- El DPD ha de ser nombrado atendiendo a sus cualificaciones profesionales y, en particular, a su conocimiento de la legislación y la práctica de la protección de datos. Aunque no debe tener una titulación específica, en la medida en que entre las funciones del DPD se incluya el asesoramiento al responsable o encargado en todo lo relativo a la normativa sobre protección de datos, los conocimientos

jurídicos en la materia son sin duda necesarios, pero también es necesario contar con conocimientos ajenos a lo estrictamente jurídico, como por ejemplo en materia de tecnología aplicada al tratamiento de datos o en relación con el ámbito de actividad de la organización en la que el DPD desempeña su tarea.

- La designación del DPD y sus datos de contacto deben hacerse públicos por los responsables y encargados y deberán ser comunicados a las autoridades de supervisión competentes.
- La posición del DPD en las organizaciones tiene que cumplir los requisitos establecidos entre los que se encuentran:
    - total autonomía en el ejercicio de sus funciones
    - necesidad de que se relacione con el nivel superior de la dirección
    - obligación de que el responsable o el encargado faciliten al DPD todos los recursos necesarios para desarrollar su actividad

DERECHOS DEL TITULAR DE LOS DATOS

Los derechos que asisten al titular de los datos, solo pueden ser ejercidos por el mismo y se concretan en:

Procedimiento para el ejercicio

- Con carácter general, los responsables deben facilitar a los interesados el ejercicio de sus derechos, y los procedimientos y las formas para ello deben ser visibles, accesibles y sencillos.

  Se requiere que los responsables posibiliten la presentación de solicitudes por medios electrónicos, especialmente cuando el tratamiento se realiza por estos medios.
- El ejercicio de los derechos será gratuito para el interesado, excepto en los casos en que se formulen solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas, el responsable podrá cobrar un canon que compense los costes administrativos de atender a la petición o negarse a actuar (el canon no podrá implicar un ingreso adicional para el responsable, sino que deberá corresponderse efectivamente con el verdadero coste de la tramitación de la solicitud).

Obligaciones para el responsable del fichero

- Articular procedimientos que permitan fácilmente que los interesados puedan acreditar que han ejercido sus derechos por medios electrónicos (actualmente, en muchas ocasiones, no es viable).
- El responsable debe demostrar el carácter infundado o excesivo de las solicitudes que tengan un coste para el interesado.
- El responsable deberá informar al interesado sobre las actuaciones derivadas de su petición en el plazo de un mes (podrá extenderse dos meses más cuando se trate de solicitudes especialmente complejas y deberá notificar esta ampliación dentro del primer mes).
- Si el responsable decide no atender una solicitud, deberá informar de ello, motivando su negativa, dentro del plazo de un mes desde su presentación.

- Los responsables deberán tomar medidas para verificar la identidad de quienes soliciten acceso y de quienes ejerzan los restantes derechos.
- El responsable que trate una gran cantidad de información sobre un interesado podrá pedir a éste que especifique la información a que se refiere su solicitud de acceso.
- El responsable podrá contar con la colaboración de los encargados para atender al ejercicio de derechos de los interesados, pudiendo incluir esta colaboración en el contrato de encargo de tratamiento.

Derecho al acceso

2. El afectado tiene derecho a solicitar y obtener información de sus datos incluidos en ficheros.

   Ello quiere decir que puede solicitarnos toda la información, tanto si está en papel como en los sistemas informáticos.

3. La información será remitida al afectado por e-mail, fax o correo certificado, pudiendo dejar siempre constancia del envío de la misma y si fuese posible se entregará personalmente y se procederá a la revisión de los datos con el cliente.

   En cualquier caso deberá quedar constancia de que ha sido remitida la documentación al cliente, por lo que en caso de entregárselo en mano deberá quedar constancia conforme se le ha entregado la misma

4. La información que se proporcione será legible e inteligible.

   Esto quiere decir que para alguien que no conoce nuestros sistemas la información debe ser comprensible, por lo que no le entregaremos ficheros

5. Los responsables podrán atender a este derecho facilitando el acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales

En un derecho al que la empresa no puede oponerse y siempre que sea solicitado debe de atenderse la petición del afectado.

Derecho de rectificación y cancelación

1. Si los datos son inexactos o incompletos, inadecuados o excesivos el afectado puede solicitar su rectificación o cancelación.

   Esto supone que si un cliente considera

   - Que los datos que tenemos son erróneos
   - Que los datos que tenemos en el fichero son excesivos para el encargo que nos realizo
   - Que los datos están incompletos

   Puede requerirnos

   - Que modifiquemos aquellos que son inexactos o erróneos
   - Que cancelemos aquellos datos que considera excesivos
   - Que cancelemos todos los datos, en el supuesto en que considere que todos son excesivos.

2. La solicitud de rectificación señalará el dato erróneo y la rectificación a realizar.

3. En la cancelación el afectado deberá indicar si revoca el consentimiento otorgado, si procede la revocación o si se trata de un dato erróneo inexacto, deberá acompañar la documentación justificativa.

4. La cancelación no procederá cuando los datos sobre los que se pida la cancelación correspondan a una relación contractual vigente o bien cuyo plazo legal de posible efecto no haya llegado a término. Igualmente la cancelación no procederá cuando pueda causar perjuicio a intereses legítimos propios o de terceros al deber de conservarse los datos.

   En los casos en que la cancelación o rectificación no proceda, deberemos comunicárselo por escrito al afectado, indicándole las causas por las que no procede.

   Si un cliente nos solicita la cancelación total de sus datos, existiendo contratos en vigor, deberemos darle a conocer esta circunstancia, indicándole que no podemos

proceder a la cancelación de los datos hasta no haber finalizado la relación contractual.

De igual manera, en los supuestos en que el cliente nos solicite la cancelación total y existan documentos sobre los que tengamos responsabilidades vigentes, o bien puedan ser objeto de auditoría contable, deberemos comunicar al afectado que no procede la cancelación total por existir obligaciones legales de conservarlos.

5. La cancelación exigirá el borrado físico de los datos del fichero.

   Si lo que queremos es mantener los datos a efectos estadísticos en nuestra base de datos, lo que deberemos realizar es eliminar todos los datos de la misma que nos permitan la identificación del cliente (nombre, NIF, Dirección), y mantendremos los restantes datos en un código de cliente que no permita la identificación de la persona.

Derecho al olvido

1. No está considerado un derecho autónomo o diferenciado de los clásicos derechos, sino la consecuencia de la aplicación del derecho al borrado de los datos personales.

   Es una manifestación de los derechos de cancelación u oposición en el entorno online

2. El denominado 'derecho al olvido' es la manifestación de los tradicionales derechos de y cancelación y oposición aplicados a los buscadores de internet. El 'derecho al olvido' hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparada

3. Los responsables que hayan hecho públicos los datos personales deberán adoptar medidas técnicas para informar a otros responsables de la solicitud del interesado de borrar su información personal

Derecho a la limitación del tratamiento

1. La limitación de tratamiento supone que, a petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían.

   Se puede solicitar la limitación cuando

   - El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender a la solicitud.
   - El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello.
   - Los datos ya no son necesarios para el tratamiento, que también determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

2. En el tiempo que dure la limitación, el responsable sólo podrá tratar los datos afectado más allá de su conservación:

   - Con el consentimiento del interesado
   - Para la formulación, el ejercicio o la defensa de reclamaciones
   - Para proteger los derechos de otra persona física o jurídica
   - • Por razones de interés público importante de la Unión o del Estado miembro correspondiente

Derecho a la portabilidad de los datos

1. Este derecho permite a los interesados recibir los datos personales que han proporcionado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable del tratamiento sin impedimentos. Este derecho, que se aplica bajo determinadas condiciones, respalda la elección, el control y la capacitación de los usuarios.

2. Derecho a recibir datos personales

   La portabilidad de los datos es el derecho del interesado a recibir un subconjunto de datos personales que le conciernan, procesados por un responsable del tratamiento, y a almacenar dichos datos para un uso personal posterior. Dicho almacenamiento podrá realizarse en un dispositivo privado o en una nube privada, sin tener que transmitir necesariamente los datos a otro responsable del tratamiento.

3. Derecho a transmitir datos personales de un responsable del tratamiento a otro responsable del tratamiento

   Los datos pueden transmitirse también directamente de un responsable del tratamiento a otro a petición del interesado y cuando sea técnicamente posible. A este respecto, la legislación alienta a los responsables del tratamiento a crear formatos interoperables que permitan la portabilidad de los datos pero sin obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles

4. Responsabilidad

   La portabilidad de los datos garantiza el derecho a recibir los datos personales y a tratarlos de acuerdo con los deseos del interesado

   Los responsables del tratamiento que responden a solicitudes de portabilidad de datos, actúan en nombre del interesado, incluso cuando los datos personales se transmiten directamente a otro responsable del tratamiento. En este sentido, el responsable del tratamiento no es responsable del cumplimiento de la legislación sobre protección de datos por parte del responsable del tratamiento que recibe los datos, habida cuenta de que él no decide quién los recibe. Al mismo tiempo, el responsable debe establecer garantías que aseguren que verdaderamente actúa en nombre del interesado. Por ejemplo, puede establecer procedimientos que garanticen que el tipo de datos personales transmitidos son efectivamente los que el interesado quiere transmitir. Esto podría hacerse obteniendo confirmación por parte del interesado, bien antes de la transmisión o aún con anterioridad, cuando se otorga el consentimiento inicial para el tratamiento o cuando se finaliza el contrato.

5. La portabilidad de los datos frente a otros derechos de los interesados

   Cuando una persona ejerce su derecho a la portabilidad de los datos lo hace sin perjuicio de ningún otro derecho (como es el caso de cualquier otro derecho contemplado en la normativa).

   Un interesado puede seguir usando el servicio del responsable del tratamiento y beneficiándose de él incluso después de una operación de portabilidad de datos. La portabilidad de los datos no conlleva su supresión automática de los sistemas del responsable del tratamiento, ni afecta al periodo de retención original aplicable a los datos que se han transmitido. El interesado puede ejercer sus derechos en tanto el responsable de los datos siga tratándolos
6. Qué datos personales deben incluirse

   Los datos deben ser:

   - -datos personales que incumban a la persona en cuestión y
   - -que esta haya facilitado a un responsable del tratamiento.

Derecho de oposición

El ciudadano puede oponerse mediante su solicitud a que sus datos sean tratados con fines de publicidad y de prospección comercial

LAS SANCIONES

Para la empresa

La protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes.

Las **Sanciones previstas** para los casos de incumplimiento son lo suficientemente importantes como para tratar de cumplir estrictamente esta Ley de Protección de Datos.

Con carácter general la normativa prevé la posibilidad de sancionar las infracciones cometidas con respecto al tratamiento de datos de carácter personal con multas administrativas de 10.000.000 o 20.000.000 de euros, o en el caso de que se trate de una empresa, de una cuantía equivalente al 2% o al 4% como máximo del volumen de negocio anual global del ejercicio financiero anterior, optándose por la de mayor cuantía

Para los trabajadores

La trasgresión por el trabajador de cualquiera de las obligaciones contenidas en el presente documento de seguridad será considerada falta muy grave en el ámbito laboral, aplicándose el régimen disciplinario previsto en el Real Decreto Legislativo 1/1995, del Estatuto de los Trabajadores, el convenio colectivo aplicable a la compañía o, en su defecto, el régimen disciplinario del Acuerdo de Cobertura de Vacíos, todo ello sin perjuicio de las acciones judiciales que pudiere ejercitar la empresa.

OBLIGACIONES DEL PERSONAL

Es responsabilidad de todos cumplir con las obligaciones de protección de datos, habiendo establecido la empresa las siguientes obligaciones

Las obligaciones de todo el personal de la correduría son:

1. El trabajador se compromete a cumplir en todo momento con sus deberes básicos de fidelidad para con la correduría, en concreto, a guardar secreto y no divulgar ni utilizar en provecho propio o de terceros cualquier clase de información o documentación de la que hubiera tenido conocimiento en razón de su trabajo para la empresa, tanto a través de medios internos, como facilitados por las entidades aseguradoras.

   Así mismo el trabajador se compromete a utilizar los sistemas informáticos, programas y medios de comunicación, internos y externos, únicamente para los fines propios de su puesto de trabajo, facultando a la empresa para el examen de los archivos y de los correos electrónicos de todo tipo contenidos en los sistemas.

   Igualmente se compromete, en lo que atañe, a observar las previsiones contenidas en la Ley de Regulación del tratamiento automatizado de los datos de carácter personal.

2. El personal no dará a conocer ni interna, ni externamente sus claves de acceso al sistema.

3. Todos los integrantes de la empresa tienen la obligación de informar a los titulares de los datos personales de los derechos de acceso, rectificación y cancelación de datos que les asiste según la Ley de Protección de Datos, lo que se realizará :

   a. Para las comunicaciones telefónicas, para clientes para los que no existe el consentimiento, se les informará del mecanismo por el que se les remitirá el documento de consentimiento y la necesidad de que firmen el mismo.

   b. Para las visitas in-situ mediante documento específico que firmará el cliente de consentimiento

   c. Para comunicaciones por correo: mediante texto informativo de la existencia de los ficheros y los derechos sobre los mismos y adicionalmente en el envío de nuevos contratos se incorpora el documento de consentimiento, en el que se informa con mayor detalle, requiriendo su firma.

   d. En las páginas web: mediante la nota legal y la política de privacidad, incorporándose un apartado específico referente a la protección de datos.

4. El personal solo accederá a la información de las personas cuando así lo requieran las tareas realizadas en cada momento.

5. La contraseña deberá ser modificada por el propio usuario con carácter trimestral, derivándose la imposibilidad de uso del sistema en caso de incumplimiento de esta norma.

   Se evitarán nombres comunes, números de matrículas de vehículos, teléfonos, nombres de familiares, amigos, etc. Y derivados del nombre del usuario como permutaciones o cambios de orden de las letras, transposiciones, repeticiones de un único carácter, etc.

   No se accederá al sistema utilizando el identificador o contraseña de otro usuario. La responsabilidad de cualquier acceso utilizando un identificador determinado, recaerá sobre el usuario que le tenga asignado.

6. Cualquier soporte informático que sea recibido en la correduría y contenga datos personales, deberá ser registrado en el Registro y autorización entrada/salida de soportes. Una vez procesado, el soporte recibido deberá ser borrado completamente. En el caso, en que por algún motivo justificado, se desee conservar el soporte recibido, deberá catalogarse, siguiendo lo establecido en el documento de seguridad.

7. La salida de soportes informáticos y ordenadores que contengan datos personales fuera de la organización, precisa de autorización y serán siempre registrados en Registro de salida de soportes, registro que se conservará por el responsable de seguridad y se mantendrá por un periodo mínimo de tres años.

   Respecto a los portátiles, se mantendrá únicamente el registro de los mismos como parte del inventario informático, indicando la persona que tiene acceso al mismo. En dichos equipos no se mantendrán ni ficheros temporales, ni documentos que mantengan datos personales, siendo la finalidad de los mismos conectarse a los equipos o servidores remotos en los que se mantienen los datos con niveles de seguridad alto.

8. Toda incidencia en materia de seguridad deberá de comunicarse siguiendo las instrucciones del documento de seguridad (apartado Incidencias).

9. Todos los ficheros temporales que los usuarios mantengan en sus equipos personales deberán ser borrados una vez finalice la tarea para la que fueron creados.

10. Queda prohibida la creación de ficheros que supongan el tratamiento de datos personales, así como la cesión sin previa autorización del responsable de protección de datos.

11. Todos los usuarios mantendrán un protector de pantalla con contraseña que se activará a los diez minutos de inutilización del sistema, no debiendo bajo ningún concepto comunicar la contraseña a otro integrante de la empresa o a personas ajenas a la misma.

12. Puestos de trabajo

    Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.

    Esto implica que tanto las pantallas como las impresoras u otro tipo de

dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse saliendo de la aplicación o programa (cuando para volver a entrar y acceder a cualquier fichero se requiera el correspondiente código de usuario y contraseña) o a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará entrar nuevamente en la aplicación o programa o bien la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

13. Impresoras

En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de los ficheros, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

14. Redes o sistemas exteriores

Queda expresamente prohibida la conexión a redes o sistemas exteriores privados de los puestos de trabajo desde los que se realiza el acceso a los ficheros, salvo los estándares definidos en el puesto de trabajo (Intranet, red corporativa y sistemas bancarios autorizados). La revocación de esta prohibición será autorizada por el responsable de los ficheros, quedando constancia de esta modificación en el registro de incidencias.

15. Configuración del puesto de trabajo

Los puestos de trabajo desde los que se tiene acceso a los ficheros tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser cambiada bajo la autorización del responsable de seguridad o por administradores autorizados.

16. Software y equipamiento

Queda prohibida la instalación de cualquier software no facilitado expresamente por el administrador del sistema. Si cualquier usuario precisa de un software específico para el desarrollo de sus funciones, lo deberá poner en conocimiento del administrador del sistema para que, a la vista de dichas necesidades, resuelva sobre la idoneidad o no de su instalación.

Todo el equipamiento de microinformática se deberá solicitar al administrador del sistema. Asimismo, su instalación deberá ser exclusivamente realizada por el administrador del sistema.

17. Correo electrónico

La finalidad de los mensajes de correo electrónico interno y a través de Internet es única y exclusivamente laboral. No se permite el uso de correo electrónico de la compañía para finalidades particulares o de ocio. Se debe tener en cuenta que este tipo de mensajes, además de poder incorporar virus, puede ocupar mucho

espacio en el servidor de correo y pueden reducir gravemente la velocidad de la conexión con Internet.

Todos los ordenadores personales de la compañía tendrán instalado un software antivirus que no puede ser reconfigurado ni desactivado por los usuarios.

No se abrirán mensajes de correo electrónico de origen desconocido o sospechoso. En caso de duda se debe consultar con el administrador del sistema.

En el supuesto de detección de virus, se debe contactar con el administrador del sistema lo antes posible.

Bajo ningún concepto y sin previa autorización del responsable del fichero se remitirá un mismo e-mail a más de un destinatario externo a la empresa. En caso de ser autorizado se enviarán siempre con la dirección de los destinatarios con copia oculta.

Nunca en el cuerpo principal de un e-mail se proporcionarán los datos personales, excepto los relativos a nombre y apellidos.

Siempre que se remitan documentos adjuntos por e-mail con datos personales, se enviarán con contraseña, remitiendo al destinatario en e-mail diferente la contraseña de apertura. Para aquellos titulares de datos personales para los que este sea el método habitual de contacto, se les remitirá una contraseña por defecto la que será siempre utilizada en los envíos a los mismos.

Todos los correos electrónicos incorporaran la siguiente cláusula al pie de los mismos

“La información contenida en el presente mensaje es confidencial y únicamente el destinatario está autorizado a leerla.

Queda prohibida la reproducción, publicación, divulgación, total o parcial del mensaje, así como el uso no autorizado por el emisor. Si este mensaje le hubiera llegado por error, elimínelo y notifique inmediatamente al remitente. Gracias por su colaboración”.

18. Destrucción de documentos

Todos los documentos que contengan datos personales y deban ser eliminados de manera segura, para lo que se utilizará o destructora de papel o empresas seguras de destrucción de papel.

19. Tratamiento de la información

En ningún caso se proporcionará información o cualquiera otro tipo de documentación a terceras personas, ajenas al titular de los datos si no se ha firmado la autorización previa.

Como excepción a lo anterior se establece, la información a trasladar que se precise para la gestión de los contratos de los clientes o la requerida por organismos oficiales como la agencia tributaria o la seguridad socia

Únicamente se proporcionará información o documentación a terceras personas, ajenas al titular de los contratos, cuando el titular de los contratos haya

autorizado expresamente a otras personas, autorización que se conservará archivada y deberá venir firmada por el titular de los contratos y acompañada de fotocopia del DNI.

En las comunicaciones telefónicas, deberá identificarse al titular del contrato de forma fehaciente, para ello se solicitará al menos el nombre, el DNI, y otro dato relevante previa comunicación de información. En caso de no ser posible la identificación se propondrá al interlocutor el envío de la información por medio del correo o el e-mail que para el mismo estén informados en el sistema.