Cuaderno Informativo
Sobre Protección de Datos

APDCM

Agencia de Protección de Datos
de la Comunidad de Madrid

Comunidad de Madrid

Cuaderno Informativo de Protección de Datos

Impreso en España
Producción Gráfica: xxxxxxxxxxxxx
Diseño y Maquetación: PRINTERALIA, S.L.
Pablo Lecroisey

Depósito Legal: M-xxxxxxxxxxxxx

Índice

Este Cuaderno que tengo la satisfacción de presentar trata de ser una aproximación a la protección de los datos personales orientada y dirigida a los menores. Estos en muchas ocasiones ceden sus datos personales en colegios, bibliotecas, instalaciones deportivas, discotecas, centros de idiomas, campañas de promoción de productos, etc, y deben ser conscientes de que sus datos tienen un valor y que un uso o cesión abusiva puede afectar a su intimidad personal y familiar.

El conocimiento de los principios de protección de datos personales y de los derechos irrenunciables que les asisten a los titulares de los datos es el primer paso para poder ejercerlos y exigirlos. Además, hay que ser consciente del valor de mis datos personales y de su posterior utilización, teniendo la necesaria diligencia y cuidado sobre los mismos, de forma que si consiento en que se traten mis datos, lo haga de una manera consciente y justificada.

Hemos tratado de exponer en este Cuaderno los aspectos fundamentales del derecho a la protección de datos, también denominado derecho a la autodeterminación informativa, de una manera sencilla, huyendo de tecnicismos y con un lenguaje claro y comprensible. Para ello, hemos aportado ejemplos que puedan ser ilustrativos para el público más joven.

Corresponde a la Agencia de Protección de Datos de la Comunidad de Madrid garantizar la efectividad de este derecho fundamental en los ficheros públicos del territorio de nuestra Comunidad. El esfuerzo para alcanzar la vigencia de este derecho fundamental a la protección de los datos personales no se debe apoyar únicamente en una actividad de inspección y de control. El mayor respeto a este derecho depende, en gran medida, del grado de concienciación de los ciudadanos acerca de su derecho fundamental a la protección de sus datos personales, y de la sensibilidad de los responsables de los ficheros y de todas las personas que tratan datos personales en el cumplimiento de sus deberes. Esta concienciación se alcanza, fundamentalmente, a través de la formación y de la transmisión de conocimiento.

Con este Cuaderno, la Agencia pretende extender la cultura de la protección de los datos personales, de manera que se integre progresivamente en la vida diaria de los ciudadanos, especialmente, entre los más jóvenes. La Agencia de Protección de Datos de la Comunidad de Madrid desarrolla, así, una labor de prestación y promoción de este derecho fundamental de forma que el hecho diferencial de nuestra Comunidad Autónoma sea el servicio a los ciudadanos y la protección de los derechos, en este caso, de la libertad informática y del derecho a la intimidad.

D. Antonio Troncoso Reigada
Director de la APDCM

APDCM

Agencia de Protección de Datos
de la Comunidad de Madrid

¿Qué es la protección de datos?

APDCM

Agencia de Protección de Datos
de la Comunidad de Madrid

¿QUÉ ES LA PROTECCIÓN DE DATOS?

Es el derecho que tienen todos los ciudadanos a que sus datos personales no sean utilizados por parte de terceros sin la autorización debida. Se trata de evitar que, a través de un tratamiento automatizado o manual, se pueda llegar a confeccionar información identificable con el titular de los datos que pueda afectar a su intimidad, a su entorno social o profesional.

Es un derecho fundamental consistente en el ejercicio de control por parte del titular de los datos sobre quien, cómo, para qué, dónde y cuándo son tratados los datos relativos a su persona. Este control se hace efectivo a su vez a través del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Su carácter de derecho fundamental, según jurisprudencia del Tribunal Constitucional, viene determinado por su ubicación en nuestra Constitución Española (CE), en el artículo 18.4, junto con el derecho fundamental al honor, la intimidad personal y familiar y la propia imagen, a la inviolabilidad del domicilio y al secreto de la correspondencia y las telecomunicaciones, aunque no se identifique literalmente este artículo con el enunciado: "derecho a la protección de datos".

Es el derecho que tienen todos los ciudadanos a que sus datos personales no sean utilizados por parte de terceros sin la autorización debida.

El artículo 18.4 de la Constitución Española dice:

"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".

Ante un masivo uso de la informática, el legislador constitucional advirtió el riesgo que el uso de estas técnicas, especialmente cuando se tratan datos personales, podía suponer para los derechos de las personas y especialmente de su intimidad. El desarrollo legislativo del mandato constitucional, contenido en el artículo 18.4, ha dado lugar a la creación de un derecho específico, el derecho a la protección de datos, derecho que ha sido también desarrollado en el ámbito europeo con plena identidad.

¿Qué consecuencias se derivan de la cualidad de derecho fundamental?

Es un derecho irrenunciable del individuo, igual que el derecho a la dignidad de la persona, el derecho a la vida, el derecho a la educación, o el derecho a la libertad, entre otros.

Su desarrollo debe hacerse a través de Ley Orgánica, requiriendo para su aprobación mayoría absoluta del Congreso de los Diputados.

Prevalece sobre el ejercicio de otros derechos no fundamentales, como el derecho a la libertad de empresa, por ejemplo.

Tiene una protección reforzada, pudiendo ejercitarse ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad, y a través del recurso de amparo ante el Tribunal Constitucional (artículo 53 CE).

APDCM

Agencia de Protección de Datos
de la Comunidad de Madrid

Regulación actual del derecho fundamental a la protección de datos

APDCM

Agencia de Protección de Datos
de la Comunidad de Madrid

REGULACIÓN ACTUAL DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

El mandato contenido en el artículo 18.4 de la CE al que nos hemos referido fue desarrollado en primer lugar por la LORTAD, Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de Datos de Carácter Personal. Actualmente esta Ley ha sido derogada y sustituida por la **LOPD, Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal**, norma de mayor rango que regula el Derecho a la Protección de Datos.
Para entender adecuadamente en qué consiste este derecho es necesario hacer un repaso del contenido de la LOPD.

Definiciones fundamentales contenidas en la LOPD:

Datos de carácter personal

Cualquier información asociada a una persona identificada o identificable.

Por persona debe entenderse únicamente la persona física o ciudadano, el ser humano individual. A través de la legislación de protección de datos no pueden protegerse los datos relativos a personas jurídicas.

Por Identificable debe entenderse toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social (artículo 2 a) de la Directiva 95/48/CE).

Más específicamente, dato identificable debe considerarse toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable (artículo 1.4 del Real Decreto 1332/1994)

Cualquier dato que nos permita identificar a una persona debe considerarse como personal, aunque en sí mismo no aparente una identificación con persona concreta. De este modo, debe considerarse dato personal el D.N.I., el número de Cuenta bancaria, o el número de carné de una biblioteca, por ejemplo.

Fichero

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

En esta definición debemos encuadrar no sólo los ficheros informatizados sino también aquellos ficheros manuales en los que su organización permita la localización de personas a través de datos personales como el nombre, apellidos, número de matrícula, etc.

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.

Dentro de la definición de tratamiento debe entenderse también el manual, es decir, cuando los datos son archivados o manejados sin la utilización de medios electrónicos o telemáticos.

Por lo tanto, cada vez que se recogen datos para confeccionar las listas de alumnos, o para saber las personas que atenderán a un determinado programa cultural, o los padres o tutores miembros de algún tipo de asociación, se está procediendo a un tratamiento de datos. Del mismo modo, cuando se envían felicitaciones por Navidad o se remite alguna comunicación al domicilio, se está realizando un tratamiento de datos.

Afectado o interesado

Persona física o ciudadano a la que hacen referencia los datos tratados. Esta persona se constituye en la titular de los datos personales, única con capacidad para prestar consentimiento al tratamiento de sus datos.

Como hemos dicho, la protección de datos se predica respecto del ciudadano. Todo ciudadano tiene este derecho elevado a la categoría máxima de derecho fundamental en nuestro Ordenamiento.

Así, cada uno de los alumnos de un centro educativo tienen el derecho fundamental a la protección de sus datos respecto del tratamiento que se haga de ellos, aunque pueda ser ejercido por sus tutores en casos de minoría de edad.

También son titulares del derecho a la protección de sus datos los profesores, los padres de los alumnos, y el personal que pertenezca al centro, respecto del tratamiento que se haga de ellos en el centro educativo.

Consentimiento

Manifestación de voluntad libre, específica e informada del afectado o interesado permitiendo el tratamiento de sus datos personales. El consentimiento del titular de los datos es fundamental para la legitimidad del tratamiento.
Existen, en Derecho, distintas clases de consentimiento. Sólo vamos a hablar de dos: el tácito y el expreso.
Por consentimiento tácito se entiende aquél que se presta cuando no se dice nada pero se sobreentiende que se da. Pongamos un ejemplo de consentimiento tácito: "si vd no nos contesta a esta carta en el plazo de un mes diciéndonos lo contrario, entendemos que tenemos su consentimiento para enviarle publicidad". Este tipo de consentimiento, en gran parte de las ocasiones, salvo las excepciones que veremos después, es válido legalmente hablando, aunque, tiene el gran problema de la prueba a efectos jurídicos.
El consentimiento expreso, por su parte, es el que se contesta, en un sentido u otro, puede prestarse de forma verbal o por escrito. El consentimiento expreso de palabra vuelve a tener problemas de prueba salvo que se prevean otros medios de prueba, como la grabación de las conversaciones, muy utilizado en la Banca telefónica.

El consentimiento del titular de los datos es fundamental para la legitimidad del tratamiento.

Responsable del fichero

Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decide sobre la finalidad, contenido y uso del tratamiento.
Es el responsable del fichero ante quien se ejercitan los derechos de acceso, rectificación, cancelación y oposición por parte de los interesados o afectados.
Esta figura, junto con el encargado de tratamiento que luego veremos, son los únicos sujetos al régimen de sanciones que regula la LOPD. Ello no quiere decir que sean los únicos que deben someterse a los principios que impone la normativa para el tratamiento de datos, todas las personas que intervienen en éste deben cumplir la legislación sobre protección de datos personales.

Cualquier persona que trate datos de carácter personal tiene que cumplir con todas las obligaciones establecidas en la normativa sobre protección de datos. Existen excepciones como la de tratar datos únicamente con fines domésticos, o la gestión de la agenda que todos tenemos con fines personales propios, por ejemplo.

Se denomina responsable del fichero porque responde de su tratamiento: los bancos, los colegios, los ayuntamientos, las bibliotecas, los clubes y asociaciones deportivas, los gimnasios, los supermercados, los institutos de idiomas o los centros de actividades extra escolares son, entre otros ejemplos, responsables del fichero cuando deciden crear y poner en funcionamiento éste para el tratamiento y gestión de los datos de sus clientes, sus alumnos, los ciudadanos, los lectores, los asociados, etc.

Cesión de datos

Únicamente con consentimiento del interesado pueden cederse sus datos a persona o entidad distinta al responsable del tratamiento.

Cualquier revelación de datos personales contenidos en un fichero a persona o entidad distinta del titular de los datos o interesado.

Únicamente con consentimiento del interesado pueden cederse sus datos a persona o entidad distinta al responsable del tratamiento. La cesión de datos se rige por el principio de consentimiento a fin de que sea únicamente el titular de los datos (afectado o interesado) el que tenga el control sobre los mismos. Tanto el que cede los datos como el que los recibe están sujetos a un requisito, que la cesión se realice para el cumplimiento de fines relacionados con las funciones legítimas de ambos.

Cuando una empresa solicita a un Centro docente los datos de sus alumnos para realizar una campaña de promoción de ropa deportiva, el Centro no podrá comunicar los datos de éstos sin su consentimiento previo o de sus representantes legales, en caso de minoría de edad.

Encargado de tratamiento

Es la persona física o jurídica, de naturaleza pública o privada que trata datos personales por cuenta del responsable del fichero.
Se trata de una excepción genérica al consentimiento del afectado para la cesión de datos.
El encargado de tratamiento está obligado por Ley a mantener un contrato con el responsable del fichero en el que se especifique el alcance del acceso a los datos personales y las medidas de seguridad del fichero.
El encargado de tratamiento está sujeto, junto con el responsable del fichero al régimen de sanciones previsto por la Ley Orgánica 15/1999.

Procedimiento de Disociación

Tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
Los datos personales disociados siguen siendo datos personales pero no permiten identificar éstos con una persona concreta. El tratamiento de estos datos de manera disociada no está sujeto a las prescripciones de la normativa sobre protección de datos porque no integra ningún riesgo para los derechos personales. Los tratamientos disociados suelen utilizarse para estudios estadísticos.

Por ejemplo, la relación de alumnos de un Centro docente nacidos en el año 1983 que ha aprobado la selectividad, sin incluir más que el año de nacimiento y la nota obtenida en ese proceso selectivo, podría constituir un fichero de datos disociados siempre que no se relacionara con ningún otro fichero que permita la identificación de cada alumno.

¿Cómo deben tratarse mis datos personales?

APDCM

Agencia de Protección de Datos
de la Comunidad de Madrid

¿CÓMO DEBEN TRATARSE MIS DATOS PERSONALES?

Hemos visto que el responsable del fichero es quien decide sobre la finalidad, contenido y uso del tratamiento de los datos personales incluidos en el fichero. Esta capacidad de decisión del responsable está sometida a determinados parámetros establecidos por la LOPD, parámetros constituidos por tres vértices fundamentales:

Los principios de protección de datos rigen todo el tratamiento, establecen los límites y las pautas a las que debe someterse todo tratamiento de datos personales para que pueda considerarse dentro de la legalidad.

Los derechos de los afectados o interesados conforman el contenido esencial del derecho fundamental a la protección de datos, son derechos irrenunciables y personalísimos, sólo pueden ejercitarse por el afectado o interesado ante el responsable del fichero.

Los procedimientos establecidos por la Ley tienen como finalidad la consecución efectiva de los derechos de los afectados estableciendo los mecanismos de reclamación ante la Agencia de Protección de Datos Estatal o Autonómica, dependiendo del ámbito competencial, y la aplicación de los principios de protección de datos, estableciendo mecanismos de control.

En conclusión, uniendo los tres vértices, los principios son las declaraciones de carácter general que exponen las reglas a cumplir en el tratamiento de datos. Pero estos principios, como todos en Derecho, se quedan sin aplicación práctica si no tienen a su lado unos derechos correlativos que sustentan su ejercicio. Y finalmente, estos derechos no tienen tampoco sentido real si, en caso de verse coartados, no tienen unos procedimientos jurídicos a los que acudir para reclamar su ejercicio.

Pongamos un ejemplo: la Constitución declara el principio a la libertad de expresión que significa que, en un Estado de Derecho como el nuestro yo tengo derecho a expresarme libremente, si este derecho me es vetado o limitado puedo acudir al procedimiento judicial previsto en las leyes para reclamar su ejercicio. Pues el derecho fundamental a la protección de datos funciona igual: existe el principio de información, yo tengo derecho a que me informen sobre el tratamiento de mis datos, y si este derecho se incumple por parte del responsable del tratamiento, puedo acudir al procedimiento ante la Agencia de Protección de Datos, para reclamar su ejercicio.

Los principios de protección de datos:

El consentimiento del afectado o interesado

Es el principio fundamental de todo tratamiento de datos. Únicamente la persona a la que se refieren los datos, titular de los mismos, es quien puede otorgar el consentimiento para que sus datos personales puedan ser incluidos en un fichero y sometidos a tratamiento. En caso de incapacidad legal o minoría de edad, el consentimiento podrá ser otorgado por el tutor legal .

El consentimiento del afectado o interesado es el principio fundamental de todo tratamiento de datos

El consentimiento es el eje sobre el que se vertebra toda la filosofía de la normativa sobre protección de datos. La mejor manera de proteger la intimidad de las personas es convirtiendo a éstas en las únicas capaces para determinar cuándo sus datos pueden ser conocidos por terceros.

No obstante, la Ley prevé excepciones a este principio cuando exista una relación negocial, laboral o administrativa entre el titular de los datos y el responsable de tratamiento, cuando sea necesario el tratamiento para proteger un interés vital, cuando se recojan para el ejercicio de funciones propias de la Administración Pública en el ejercicio de sus competencias o cuando los datos hayan sido recogidos de fuentes accesibles al público (guías telefónicas, listas de profesionales colegiados, por ejemplo).

No será necesario nuestro consentimiento cuando sea necesario tratar nuestros datos personales para atendernos de urgencia en un hospital. De igual modo, cuando un alumno es admitido en un centro educativo, se pueden tratar sus datos en tanto necesarios para el mantenimiento de la relación entre el Centro y el alumno, pero se necesitará consentimiento para tratarlos con fines que excedan esa finalidad.

Información en la recogida de datos

Cuando se recaban los datos del interesado, momento que normalmente coincide con la prestación del consentimiento, se debe informar de manera precisa e inequívoca al titular de los datos de los siguientes extremos:

- La existencia del fichero y la finalidad del tratamiento, los destinatarios de la información.
- El carácter facultativo u obligatorio de su respuesta y las consecuencias de la negativa a prestar los datos.
- La posibilidad de ejercicio de los derechos de acceso, rectificación, cancelación y oposición, y la identidad y dirección del responsable ante quien puede ejercitarlos.

Esta información debe prestarse al interesado incluso en el caso de no ser necesario la prestación del consentimiento por producirse alguna de las excepciones previstas en la Ley.

Así, por ejemplo, cuando se haga un regalo por hacerse socio de una discoteca (para lo que evidentemente se recaban datos personales), o cuando se rellene un cupón para que se envíe una muestra gratis de un producto determinado, debe informarse de todos los extremos anteriores.

Calidad de los datos

Los datos objeto de tratamiento tienen que ser pertinentes, adecuados y no excesivos en relación con las finalidades determinadas, expresas y legítimas para las que se hubieran recabado, debiendo mantenerse exactos y puestos al día y no pudiendo permanecer en el fichero más tiempo del que resulte necesario para cumplir con la finalidad para la que se registraron.

Los datos objeto de tratamiento tienen que ser pertinentes, adecuados y no excesivos en relación con las finalidades determinadas, expresas y legítimas para las que se hubieran recabado

En definitiva, la calidad de los datos implica que el responsable que los trata debe, en primer lugar, poder hacerlo no sólo porque cuente con el consentimiento (o esté en una excepción al mismo) y haya informado debidamente, sino que además debe tener en cuanta que los datos no sean excesivos en relación con la finalidad para la que se destinan. Es decir, no se pueden tratar datos que no sean necesarios para el fin del tratamiento.

Por ejemplo: no es necesario que me pregunten dónde veraneo, cuántos hermanos tengo o dónde estudio para hacerme socio de un video club.

Datos especialmente protegidos

La LOPD exige el cumplimiento de medidas especiales para el tratamiento de datos relativos a **la ideología, la afiliación sindical, la religión o creencias, el origen racial, la salud y la vida sexual**.

Esta especialidad viene determinada por la necesidad de proteger unos datos que, por la información a la que se refieren, pueden provocar la violación de otros derechos fundamentales a la vez que el propio derecho de protección de datos, como el derecho a la igualdad y no discriminación, el derecho a la libertad de pensamiento o el derecho a la libertad religiosa, entre otros. En este sentido la Ley prohíbe expresamente la creación de ficheros con la finalidad exclusiva de almacenar este tipo de datos.
En caso de ser tratados datos especialmente protegidos, también llamados sensibles, la Ley exige consentimiento expreso, y por escrito si son de ideología, afiliación sindical, religión o creencias.

Además, en el caso de comisión de infracciones, la gravedad de la misma aumenta en un grado cuando el fichero contenga datos especialmente protegidos.

Otra exigencia para los ficheros que contengan datos sensibles es la de instalar medidas de seguridad de nivel alto.

Deber de secreto

El deber de secreto respecto a los datos personales tratados es una obligación que corresponde al Responsable del fichero y a cuantos intervengan en el tratamiento. Obligación que perdura incluso finalizada la relación que permitía el acceso al fichero.

El desempeño de cualquier trabajo que nos permita el acceso a un fichero de datos personales genera automáticamente la obligación de guardar secreto respecto de los mismos, aunque sea un trabajo temporal, pongamos por ejemplo trabajos en prácticas o temporales de verano.

Por ejemplo, si como personal de un Centro tengo acceso a datos de carácter personal contenidos en los ficheros de esa entidad, tengo la obligación legal de guardar secreto y no transmitirlos a nadie, incluso una vez haya dejado de prestar servicios en dicha entidad. Evidentemente, no puedo contarle las calificaciones de un alumno a terceros.

Medidas de Seguridad

Se trata de otra obligación del responsable del fichero para garantizar la integridad y seguridad de los datos personales tratados. Las medidas de seguridad se prevén en la LOPD pero están desarrolladas en el Reglamento de Medidas de Seguridad (Real Decreto 994/1999). Son de índole técnica y organizativa, no sólo se trata de garantizar la seguridad del software sino de que los ordenadores estén adecuadamente instalados, no se trabaje con ellos a la vista de las personas no autorizadas para visualizarlos o no se pueda tener a ellos más accesos que los estrictamente autorizados, por ejemplo.

Las medidas de seguridad tienen distintos niveles dependiendo del tipo de datos tratados en el fichero en concreto:

- Medidas de nivel básico que deben ser cumplidas por cualquier fichero que contenga datos personales.
- Medidas de nivel medio cuando, además, los datos se refieren a infracciones administrativas o penales, a la Hacienda Pública, servicios financieros o solvencia patrimonial y crédito.
- Medidas de nivel alto previstas para todos aquellos ficheros que contengan datos especialmente protegidos o sensibles.

Las medidas de seguridad son una obligación a cumplir por todos aquellos que tratan datos de carácter personal. El responsable del fichero es el competente para determinar su implantación y los usuarios deben respetarlas y cumplirlas.

Si se tiene un sistema de contraseñas, no se pueden comunicar a un tercero o dejarlas en un lugar no seguro (por ejemplo, poner una notita pegada debajo del teclado del ordenador, o incluso en el tablón de un despacho, para que no se olvide), o dejar las pantallas de los ordenadores activas, y sin la vigilancia del usuario, a la vista de terceros.

Cesión de datos

Definida legalmente como toda revelación de datos hecha a una persona distinta del propio interesado, la cesión o comunicación de datos sólo podrá llevarse a cabo para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado, salvo que la Ley disponga lo contrario.

El control sobre mis datos implica que tengo que conocer o poder conocer quién los trata, por lo que si se ceden a un tercero distinto debo, como regla general, haberlo consentido y, en todo caso, saberlo.

En resumen, para que el responsable del fichero que trata los datos se los pueda ceder a un tercero para que los trate también, el afectado tiene que haber consentido.
Existen algunas excepciones a este principio:

- Que la cesión sea necesaria para una relación negocial, laboral o contractual que se esté desarrollando (por ejemplo, si voy a una agencia de viajes para contratar un viaje para irme al extranjero a aprender idiomas, la agencia necesitará darle los datos a la compañía aérea con la que vuele);
- Cuando la comunicación sea necesario en caso de urgencia con datos de salud (por ejemplo, si tienen que dar mis datos a otro hospital para preguntar si hay sangre de mi tipo sanguíneo para una transfusión); o
- Cuando los datos provengan de "fuentes accesibles al público" (por ejemplo, los datos que aparecen en la guía telefónica).

Acceso a datos por cuenta de tercero. El encargado de tratamiento

Ya vimos en las definiciones quien era el encargado de tratamiento. Puntualicemos aquí algunos aspectos.

La LOPD regula la relación de éste con el responsable del fichero en el artículo 12 titulado "acceso a datos por cuenta de terceros". Se trata de una excepción genérica a la exigencia de consentimiento para el acceso a datos personales de persona distinta del titular de los datos o del responsable del fichero.

El acceso en este caso tiene una determinada finalidad y está sujeta a límites concretos:
La finalidad es el cumplimiento de un determinado trabajo contratado con el responsable del fichero (mantenimiento informático, mensajería, envíos publicitarios, trabajos temporales de recogida de datos, etc.).
Los limites están en la formalización de un contrato entre encargado de tratamiento y responsable del fichero en el que se especifica cómo va a llevarse a cabo el tratamiento de datos por parte del encargado del fichero, y que éste actuará bajo la decisión del responsable del fichero.

Los derechos de los ciudadanos interesados

Dentro de los derechos incluidos bajo este título en la LOPD, debemos distinguir dos grupos, los derechos que constituyen el contenido esencial del derecho a la protección de datos, de acuerdo con la doctrina del Tribunal Constitucional, que son el derecho de acceso, rectificación, cancelación y oposición; y por otro lado el derecho a impugnación, el derecho a indemnización y el derecho a la consulta del Registro General de Protección de Datos.

El derecho de acceso

Es el derecho que tiene todo ciudadano para conocer sus datos personales que figuran en un fichero determinado sometidos a tratamiento, cuál ha sido el origen de éstos, y qué cesiones se han realizado o se prevean realizar en el futuro.

Este derecho se ejercita ante el responsable del fichero por el titular de los datos o afectado, es un derecho personalísimo que no puede ejercitarse por persona distinta de su titular, a excepción de menores e incapaces.

El derecho de acceso se ejerce mediante solicitud dirigida al responsable por cualquier medio que garantice la identificación del afectado y en la que conste el fichero o ficheros a consultar.

El responsable del fichero deberá responder en el plazo máximo de un mes contestando a los extremos solicitados.

El derecho de acceso. Es el derecho que tiene todo ciudadano para conocer los datos que sobre su persona figuran en un fichero determinado sometidos a tratamiento, cuál ha sido el origen de éstos, y qué cesiones se han realizado o se prevean realizar en el futuro.

El derecho de rectificación

Cuando el titular de los datos tuviera constancia de que sus datos personales tratados en un fichero son inexactos, incompletos, inadecuados o excesivos, podrá solicitar del responsable del fichero la rectificación de los mismos.

Este derecho se ejercita ante el responsable del fichero por el titular de los datos o afectado, es un derecho personalísimo que no puede ejercitarse por persona distinta de su titular, a excepción de menores e incapaces.

El derecho de rectificación se ejerce mediante solicitud dirigida al responsable por cualquier medio que garantice la identificación del afectado. El responsable deberá atender a la petición en el plazo de diez días

También el responsable podrá modificar por propia iniciativa los datos que resulten inexactos o incompletos.

Por ejemplo, la corrección de cualquiera de los datos personales que consten en el expediente personal de un alumno podría llevarse a cabo a través del derecho de rectificación cuando se constate que ese dato ha sido recogido erróneamente.

El derecho de cancelación

Cuando el titular de los datos tuviera conocimiento de que sus datos personales tratados en un fichero son inexactos o incompletos, inadecuados o excesivos, podrá solicitar del responsable del fichero la cancelación de los mismos.

La cancelación dará lugar al bloqueo de los datos.

Este derecho se ejercita ante el responsable del fichero por el titular de los datos o afectado. Igualmente es un derecho personalísimo sólo ejercitable por el titular de los datos o su representante legal, de manera que la solicitud deberá contener la identificación del afectado. El responsable deberá atender la petición en el plazo de diez días.

Podrá el responsable del fichero cancelar los datos cuando no se ajusten a lo dispuesto en la LOPD o cuando resulten inexactos o incompletos.

La petición de cancelación por parte del afectado está limitada por el deber de conservación de los datos durante los plazos previstos en las disposiciones aplicables o durante las relaciones contractuales con la persona o entidad responsable del tratamiento, sin perjuicio de la posible rectificación de los datos.

El derecho de oposición

En aquellos casos en los que no resulte necesario el consentimiento del interesado para el tratamiento de sus datos, y siempre que una Ley no disponga lo contrario, éste podrá oponerse al tratamiento de los mismos cuando existan motivos fundados y legítimos. El responsable del fichero tendrá que proceder a la exclusión de los datos relativos al afectado.

Por ejemplo, puedo ejercitar mi derecho de oposición para que no aparezca mi teléfono y dirección en la guía telefónica o para que mis datos registrados en el padrón municipal no formen parte del censo promocional.

Derecho de impugnación

Faculta al interesado a impugnar aquellas decisiones que tengan efectos jurídicos y cuya base sea únicamente un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

Derecho a indemnización

Es el derecho del afectado o interesado a que se le indemnice económicamente cuando a consecuencia del incumplimiento de lo dispuesto en la L.O. 15/1999 sufra daño o lesión en sus bienes o derechos.

La indemnización se solicitará ante la jurisdicción ordinaria cuando la lesión provenga de entidades privadas y mediante la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas cuando la lesión provenga de organismos públicos.

Derecho de consulta al Registro General de Protección de Datos

Se trata del derecho de los interesados o afectados a recabar información del Registro de Protección de Datos sobre la existencia de ficheros que traten datos personales, la finalidad de éstos y la identidad del responsable del fichero.

La información existente en el Registro se limita a determinadas características de los ficheros, su identificación, quién es el responsable del mismo, dónde se ubican y el tipo de datos que tratan, entre otras.

La solicitud del afectado no puede expresarse de forma genérica, es decir, no se puede solicitar la identificación de todos los ficheros donde se esté tratando nuestro nombre, apellidos, fecha de nacimiento, ...etc. El Registro no puede contestar a ese requerimiento porque no conoce el contenido de los ficheros.

Se puede solicitar por ejemplo información de los ficheros de datos que tenga en Ministerio de Educación o información sobre los ficheros de datos personales de la Concejalía de Asuntos Sociales, o información sobre los ficheros que tenga el polideportivo del barrio.

Este derecho es ejercitable también ante el Registro de Ficheros de Datos Personales perteneciente a la Agencia de Protección de Datos de la Comunidad de Madrid aunque la LOPD se refiere únicamente al Registro General de Protección de Datos, órgano incluido

dentro de la Agencia de Protección de Datos del Estado. La información, en este caso, se limitará al ámbito competencial del Órgano autonómico.

¿Sólo tengo derechos?

No. También tengo deberes, deber de diligencia y deber de cuidado sobre mis datos.

Tengo que ser consciente del valor de mis datos y su posterior utilización, y actuar en consecuencia.

Es decir, si consiento a que se traten mis datos, debo hacerlo de una manera sensata y razonada. Debo evitar comerciar con mis datos a cambio de regalos, premios o invitaciones puntuales que conllevan el consentimiento para su utilización con múltiples finalidades. Por ejemplo, cuando doy mis datos para que me envíen un CD de regalo a casa, o para entrar gratis o tomar algo en una discoteca, tengo que ser consciente de lo que estoy haciendo, y leer la cláusula informativa que debe existir para saber qué estoy consintiendo.
Como ya hemos visto, el consentimiento es la regla básica de la protección de datos, cuando lo doy estoy autorizando a quien me los pide para que efectúe tratamiento de los mismos. En muchos casos, ese consentimiento se otorga también para que puedan cederlos a terceros sin ser consciente de ello.
Es necesario pensar en lo que se está haciendo cuando se otorga el consentimiento, valorar, según los criterios de cada cuál, el "precio" de nuestros datos, porque en muchas ocasiones aportan más valor para el que los recaba que el coste del regalo que te están ofertando. El consentimiento otorgado para el tratamiento de nuestros datos debe ser una elección consciente e informada.

Procedimientos y órganos de control

Si considero que ha sido vulnerado mi derecho a la protección de mis datos personales, podré acudir ante la Agencia de Protección de Datos.

Si la vulneración proviene de un organismo público perteneciente al territorio de la Comunidad de Madrid, me dirigiré a la Agencia de Protección de Datos de la Comunidad de Madrid. Si la vulneración proviene de una entidad privada u organismo público del Estado acudiré a la Agencia de Protección de Datos del Estado.

La Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de Datos (LORTAD), primera legislación orgánica sobre protección de datos en España, previó la creación de La Agencia de Protección de Datos, como órgano de control sobre la aplicación de la Ley, y la creación de órganos similares en cada Comunidad Autónoma con competencias en su ámbito territorial.

La Agencia de Protección de Datos de la Comunidad de Madrid es la primera en el ámbito autonómico y fué prevista por la Ley 13/1995, de 21 de abril, de Regulación del uso de informática en el tratamiento de datos personales por la Comunidad de Madrid, modificada por la Ley 13/1997, de 16 de junio. Actualmente esta normativa ha sido derogada por la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid

Tanto la Agencia de Protección de Datos del Estado como la de la Comunidad de Madrid, cada una en su ámbito competencial, tienen como función el control de la aplicación de la Legislación sobre protección de datos y la defensa de los derechos previstos a los ciudadanos para el efectivo cumplimiento del derecho fundamental a la protección de datos personales.

El ejercicio de los derechos de acceso, rectificación y cancelación no satisfechos por el responsable del fichero pueden ser reclamados ante la APD correspondiente que abrirá un procedimiento de tutela de derechos a fin de determinar si estos han sido vulnerados.

Entre las funciones de las Agencias de Protección de Datos es de destacar la atención de peticiones y reclamaciones de los ciudadanos, la información sobre sus derechos, y el ejercicio de la potestad inspectora y sancionadora.

El ejercicio de los derechos de acceso, rectificación y cancelación no satisfechos por el responsable del fichero pueden ser reclamados ante la APD correspondiente que abrirá un procedimiento de tutela de derechos a fin de determinar si estos han sido vulnerados.

La Agencia de Protección de Datos de la Comunidad de Madrid tiene competencias para inspeccionar de oficio o a instancia de parte los ficheros de datos personales creados o gestionados por:

- Las Instituciones de la Comunidad de Madrid. (Ejemplo: Consejería de Educación)
- Los Órganos, Organismos, Entidades de Derecho público y demás Entes públicos integrantes de la Administración Pública de la Comunidad de Madrid. (Ejemplo: Consorcio Regional de Transportes)
- Los Entes que integran las Administración Local del ámbito territorial de la Comunidad de Madrid. (Ejemplo: Ayuntamientos)
- Las Universidades públicas del ámbito territorial de la Comunidad.(Ejemplo: Universidad Complutense)
- Las Corporaciones de derecho público representativas de intereses económico y profesionales de la Comunidad. (Ejemplo: Colegio de Abogados, Cámara de Comercio e Industria de la Comunidad de Madrid)

El objeto de las inspecciones es comprobar si se cumplen los principios de protección de datos y se respetan los derechos de los ciudadanos. En su caso, se podrá abrir el correspondiente procedimiento de infracción de Administración Pública.

Los procedimientos abiertos contra responsables de ficheros de titularidad pública podrán finalizar con la propuesta de expediente disciplinario al superior jerárquico correspondiente.

Los procedimientos sancionadores iniciados por la Agencia de Protección de Datos del Estado contra los responsables de ficheros privados podrán finalizar en sanción económica, con multas que van desde los 601,01 euros, sanción mínima por infracción leve, hasta 601.012,10 euros, sanción máxima por infracción muy grave.

Internet y la Protección de Datos

Actualmente todos utilizamos con frecuencia y facilidad Internet y sus muchas aplicaciones.

Cuando utilizo mi correo-e, participo en chats o en foros de debate, compro en un sitio web, o simplemente navego por la red, voy dejando una estela de datos personales que pueden ser recogidos y organizados. El peligro sería la creación de un perfil de mi personalidad que contenga información sobre mi persona, incluso desconocida por mí, en cuanto elaborada a partir de datos aislados y diseminados por Internet. Existen muchos dispositivos con gran valor comercial que van recogiendo información personal de gran interés.

La red abierta que es Internet aumenta los problemas con respecto a la Protección de Datos, fundamentalmente respecto a la seguridad y calidad del tratamiento, por la velocidad del mismo, las posibilidades de utilización o la intervención de distintos agentes.

Como usuarios de Internet debemos tomar una serie de precauciones añadidas cuando naveguemos por la red para evitar ir dejando un rastro de información personal que luego puede ser utilizada fuera de mi control. De un lado, existen ya unas soluciones y herramientas tecnológicas que nos ayudan a mantener el control sobre nuestra privacidad, pero, sin llegar a ellas, basta comenzar por tener una "cultura de protección de datos", y saber que debo tener una diligencia sobre el uso y el destino que le doy en cada momento a mi información personal, pues puedo estar consintiendo tratamientos que realmente no deseo por una simple falta de cuidado.

APDCM

Agencia de Protección de Datos
de la Comunidad de Madrid


APD
Agencia de Protección
de la Comunidad de Madrid
Conoces tus

Normativa

APDCM

Agencia de Protección de Datos
de la Comunidad de Madrid

NORMATIVA

- Constitución Española: arts. 18.4 y 105 b)

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. núm. 298, 14/12/1999) que deroga la Ley 5/1992, de 29 de octubre, sobre Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

- Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid (B.O.C.M. núm. 175, 25/07/2001), que deroga la Ley 13/1995, de 21 de abril, de Regulación del uso de informática en el Tratamiento Automatizado de datos personales por la Comunidad de Madrid modificada por la Ley 13/1997, de 16 de junio.

- Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (B.O.E. núm. 147, 21/6/1994) (Subsistente en virtud de la Disposición Transitoria Tercera de la Ley Orgánica 15/1999)

- Real Decreto 994/1999, de 11 de junio, por el que aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal (B.O.E. núm. 151, 25/6/1999) (Subsistente en virtud de la Disposición Transitoria Tercera de la Ley Orgánica 15/1999)

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (D.O. L 281, 23/11/1995)

- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

- Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos fundamentales de acceso, rectificación y cancelación en ficheros automatizados (B.O.E. núm. 25, 29/1/1998)

APDCM

Agencia de Protección de Datos
de la Comunidad de Madrid

Glosario de Términos

APDCM

Agencia de Protección de Datos
de la Comunidad de Madrid

GLOSARIO DE TÉRMINOS

Accesos autorizados: Autorizaciones concedidas a un usuario para la utilización de los diversos recursos (art. 2.4 R.D. 994/1999).

Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del artículo 3 LOPD (art. 3 e LOPD).

Autenticación: Procedimiento de comprobación de la identidad de un usuario (art. 2.6 R.D. 994/1999).

Bloqueo de datos: La identificación y reserva de los datos con el fin de impedir su tratamiento (art. 1.1 R.D. 1332/1994).

Comunicación o cesión de datos: Toda revelación de datos realizada a una persona distinta del interesado. (art. 3 i LOPD).

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 (art. 3 h LOPD).

Contraseña: Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario (art. 2.8 R.D. 994/1999).

Control de acceso: Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos (art. 2.7 R.D. 994/1999).

Copia de respaldo: Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación (art. 2.12 R.D.994/1999).

Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables (art. 3 a LOPD).

Declarante: Persona física que cumplimenta la solicitud de inscripción y actúa como mediador entre la Agencia y el titular/responsable del fichero. No debe necesariamente coincidir con el titular/responsable.

Destinatario: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios (art. 2 h Directiva 95/46/CE).

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 (art. 3 g LOPD).

Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso (art. 3 b LOPD).

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 (art. 3 j LOPD).

Identificación: Procedimiento de reconocimiento de la identidad de un usuario (art. 2.5 R.D. 994/1999).

Identificación del afectado: Cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona afectada (art. 1.5 R.D. 1332/1994).

Incidencia: Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos (art.. 2.9 R.D. 994/1999).

Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable (art. 3 f LOPD).

Recurso: Cualquier parte componente de un sistema de información (art. 2.3 R.D. 994/1999).

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 (art. 3 d LOPD).

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 (art. 2.11 R.D. 994/1999).

Sistema de información: Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal (art 2.1 R.D. 994/1999).

Soporte: Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos (art. 2.10 R.D. 994/1999).

Tercero: La personas física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento (art. 2 f) Directiva 95/46/CE).

Transferencia de datos: El transporte de los 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 (art. 1.6 R.D. 1332/1994).

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 (art. 3 c LOPD).

Usuario: Sujeto o proceso autorizado para acceder a datos o recursos (art. 2.2 R.D. 994/1999).