**DOCUMENTO DE SEGURIDAD**

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

MEDIDAS DE SEGURIDAD APLICADAS AL TRATAMIENTO DE DATOS PERSONALES

INDICE

Objeto

Principios Generales

Guía para el responsable de la protección de datos personales

* Medidas de protección de datos personales
* Obligaciones de información
* Ejercicio de derechos
* Gestión de riesgo y evaluación de impacto
* Actuación en caso de brechas de seguridad
* Encargado de tratamiento de datos personales
* Transferencias de datos personales con carácter internacional

Delegado de Protección de Datos Personales

Objeto

El presente documento responde a la obligación establecida en el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento y la libre circulación de datos personales, en adelante, RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales en adelante LOPDGDD.

Será obligatorio el cumplimiento de los requerimientos y obligaciones para el responsable y el encargado de tratamiento que este incluye, entre las que destaca, la necesidad de llevar a cabo un análisis de riesgos con el fin de establecer medidas de seguridad y control para garantizar los derechos y libertades de las personas.

Se presenta de forma sistemática las principales cuestiones que las organizaciones deberán tener en cuenta de cara a la aplicación del RGPD, para que resulte de ayuda a los responsables y a los encargados de tratamiento. Es posible y recomendable incorporar cualquier otra medida que se considere oportuna para aumentar la seguridad de los tratamientos, o incluso, adoptar las medidas exigidas para un nivel de seguridad superior al que por el tipo de información les corresponde, teniendo en cuenta la infraestructura y las circunstancias particulares de la organización.

Este documento contiene una guía para los responsables de tratamiento, que a su vez desarrolla las medidas adecuadas para adoptar en la organización para la correcta protección de los datos personales, así como las obligaciones legales para los responsables, el ejercicio de los derechos y la gestión de los riesgos. Asimismo, incluye las medidas adicionales en caso de realizar transferencias internacionales de datos personales o la necesidad de Delegado de Protección de Datos en la organización.

El presente documento es de aplicación tanto a las actividades de tratamiento como a los ﬁcheros que contienen datos de carácter personal que se hallan bajo la responsabilidad del Responsable del Tratamiento, tanto cuando actúa como tal o como Encargado del Tratamiento; incluyendo los sistemas de información, comunicación, soportes, equipos y resto de recursos empleados, entre los cuales queda incluido el personal, para el tratamiento de datos de carácter personal.

Principios Generales

De conformidad con el artículo 5 del Reglamento General de Protección de Datos, los principios relativos al tratamiento de datos personales son los siguientes:

1. Tratados de manera lícita, leal y transparente en relación con el interesado;
2. recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines;
3. adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados;
4. exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan;
5. 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; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos;
6. tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

El responsable del tratamiento será responsable del cumplimiento de lo dispuesto y capaz de demostrarlo

Por todo lo expuesto, es necesario tener en cuenta en relación a la protección de datos la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.

En términos prácticos, esta necesidad requiere que se analicen qué datos tratan, con qué finalidades se hace y qué tipo de operaciones de tratamiento se llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que se aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión. En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

Las principales medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas. De acuerdo con este enfoque, algunas de las medidas que el RGPD establece se aplicarán sólo cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten. La aplicación de las medidas previstas por el RGPD debe adaptarse, por tanto, a las características de las organizaciones. Lo que puede ser adecuado para una organización que maneja datos de millones de interesados en tratamientos complejos que involucran información personal sensible o volúmenes importantes de datos sobre cada afectado no es necesario para una pequeña empresa que lleva a cabo un volumen limitado de tratamientos de datos no sensibles.

Asimismo, el Reglamento General de Protección de Datos mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos necesita apoyarse en una base que lo legitime. También recoge las mismas bases jurídicas que contenía la Directiva y que reproduce la LOPD:

* Consentimiento.
* Relación contractual.
* Intereses vitales del interesado o de otras personas.
* Obligación legal para el responsable.
* Interés público o ejercicio de poderes públicos.
* Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

De este modo, en el caso de las bases jurídicas legitimadoras del tratamiento de datos personales por parte de las organizaciones privadas, podemos tener en cuenta, entre otras: relación contractual previa que contemple el tratamiento, consentimiento del ciudadano o interés legítimo que prevalezca sobre los derechos de las personas, entre otras.

Por tanto, en la actualidad, no resulta necesario que el particular consienta el tratamiento de sus datos personales si existe otra base jurídica que legitime el tratamiento.

En los casos en los que el consentimiento del ciudadano sea preciso por no existir otra base legitimadora, la Ley establece que debe ser una manifestación de voluntad libre, específica, informada e inequívoca por la que una persona acepta el tratamiento de sus datos personales, ya sea mediante una declaración o una clara acción afirmativa. Se excluye el consentimiento tácito o por omisión.

Además, cuando se pretenda que el consentimiento del ciudadano legitime un tratamiento para una variedad de finalidades, será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

No podrá denegarse un contrato o la prestación de un servicio por el hecho de que la persona no consienta el tratamiento de sus datos personales para finalidades que no guarden relación con ese contrato o con la prestación de ese servicio.

Guía para el responsable de la protección de datos personales

# Medidas de protección de datos personales

El RGPD establece un catálogo de las medidas que los responsables, y en ocasiones los encargados, deben aplicar para garantizar que los tratamientos que realizan son conformes con el Reglamento y estar en condiciones de demostrarlo.

En primer lugar, vamos a mencionar la obligación relativa a todos los responsables de realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo. El tipo de análisis variará en función de los tipos de tratamiento, la naturaleza de los datos, el número de interesados afectados y la cantidad y variedad de tratamientos que la organización lleve a cabo.

Por consiguiente, en el presente documento realizaremos una valoración de los riesgos inherentes a la organización.

Por otro lado, también se establece la obligación para los responsables y encargados de mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el RGPD y que contenga las cuestiones básicas de: nombre y datos de contacto del responsable o corresponsable, finalidades de tratamiento, descripción de categorías de interesados y categorías de datos personales tratados, así como, entre otros, transferencias internacionales de datos. Esta obligación es exigible para aquellas organizaciones que empleen a más de 250 trabajadores, no obstante, es recomendable utilizar esta medida para prevenir los riesgos que puedan alcanzar a los derechos y libertades de los interesados.

Se debe considerar también la obligación de notificar las violaciones de seguridad de los datos. El RGPD define las violaciones de seguridad (o como también se las conoce “quiebras de seguridad”), de una forma muy amplia, que incluye todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

Cuando se produzca una violación de seguridad de los datos, el responsable debe 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.

Por último, debemos tener en cuenta la obligación para los responsables de tratamiento de realizar una evaluación de impacto sobre la protección de datos. Esta evaluación deberá hacerse 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. La finalidad de realizar esta evaluación es determinar las necesidades adicionales en materia de protección de datos, pues si se llevan a cabo tratamientos de datos a gran escala o bien tratamiento de datos sensibles o que conlleven efectos jurídicos relevantes, supondría la necesidad de adoptar la figura en la organización de un Delegado de protección de datos.

# Obligaciones de información

Todas las organizaciones quedan obligadas a informar a los ciudadanos de forma clara y sencilla sobre los aspectos más importantes del tratamiento de sus datos, identificando quién trata los datos, con qué base jurídica, para qué finalidad, y sobre la forma de ejercer los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición y decisiones automatizadas.

Las organizaciones no podrán denegar el ejercicio de estos derechos en el caso de que el ciudadano quiera ejercitarlos de un modo diferente al que se le ofrezca.

La obligación de informar a las personas interesadas sobre las circunstancias relativas al tratamiento de sus datos recae sobre el Responsable del Tratamiento.

La información se debe poner a disposición de los interesados en el momento en que se soliciten los datos, previamente a la recogida o registro, si es que los datos se obtienen directamente del interesado.

En el caso de que los datos no se obtengan del propio interesado, por proceder de alguna cesión legítima, o de fuentes de acceso público, el Responsable informará a las personas interesadas dentro de un plazo razonable, pero, en cualquier caso: antes de un mes desde que se obtuvieron los datos personales; antes o en la primera comunicación con el interesado; o antes de que los datos, en su caso, se hayan comunicado a otros destinatarios. Esta obligación se debe cumplir sin necesidad de requerimiento alguno, y el responsable deberá poder acreditar con posterioridad que la obligación de informar ha sido satisfecha.

La información a las personas interesadas debe proporcionarse con un lenguaje claro y sencillo, de forma concisa, transparente, inteligible y de fácil acceso.

Se debe ofrecer la identidad del Responsable del Tratamiento, así como los datos de contacto del mismo, entendiéndose por éstos la dirección postal y la dirección electrónica.

Debe informarse también de los fines del tratamiento a que se destinan los datos personales, incluyendo el plazo durante el cual se conservarán dichos datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo. Debe tenerse en cuenta que, los fines deberán ser determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

Asimismo, se indicará la base jurídica en la cual se basa el tratamiento, según sea: por ejecución de un contrato, por cumplimiento de una obligación legal, o en interés público o ejercicio de Poderes Públicos, así como también por propio consentimiento del interesado.

Cuando se haya previsto ceder o comunicar, legítimamente, los datos personales que se recogen, se informará acerca de la identidad de los destinatarios, si están claramente determinados, o de las categorías de destinatarios, si estos no están determinados previamente.

El Responsable informará claramente sobre cómo podrá ejercer el interesado materialmente los derechos de acceso, rectificación o supresión, limitación, oposición o portabilidad del tratamiento de los datos personales. Deberá informar también de que los interesados podrán presentar una reclamación ante la Autoridad de Control en materia de Protección de Datos competente.

Para el efectivo cumplimiento de estas previsiones legales, habilitamos una serie de instrumentos de los que debe hacer uso en la organización con la finalidad de evitar las posibles sanciones por incumplimiento. (*en Anexos Prácticos de la documentación*)

# Ejercicio de derechos

Los responsables deben facilitar a los interesados el ejercicio de sus derechos, y los procedimientos y las formas para ello deberán ser visibles, accesibles y sencillos.

El ejercicio de los derechos será gratuito para el interesado, excepto en los casos en los 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.

De modo que se establecen como obligaciones para los Responsables del Tratamiento:

* Articular procedimientos que permitan fácilmente que los interesados puedan acreditar que han ejercido sus derechos por medios electrónicos
* Demostrar el carácter infundado o excesivo de las solicitudes que tengan un coste para el interesado.
* Informar al interesado sobre las actuaciones derivadas de su petición en el plazo de un mes (podrá extenderse a dos meses más cuando se trate de solicitudes especialmente complejas y deberá notificar esta ampliación dentro del primer mes)
* Si decide no atender una solicitud, deberá informar de ello, motivando su negativa, dentro del plazo de un mes desde su presentación.
* Adoptar medidas para verificar la identidad de quienes soliciten el acceso y de quienes ejerzan los restantes derechos
* 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.

Por todo lo expuesto, la normativa de protección de datos permite que se puedan ejercer los derechos de acceso, rectificación, oposición, supresión (“derecho al olvido”), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas.

DERECHO DE ACCESO

El derecho de acceso se define como el derecho que tiene toda persona a obtener información sobre el tratamiento de sus datos personales.

Se trata de un derecho personalísimo, pudiendo ejercerse solamente por el interesado, es decir, el titular de los datos personales.

El Responsable del tratamiento debe ofrecer en su política de privacidad la información sobre cómo pueden ejercer los interesados sus derechos ARCO (ARSULIPO) en general, y el derecho de acceso en particular.

A continuación, se facilita el formulario de solicitud de acceso a los datos personales y de denuncia ante la AEPD en caso de denegación de acceso, así como un modelo con la posible respuesta del mismo, en los *Anexos Prácticos.*

DERECHO DE RECTIFICACIÓN

El derecho de rectificación es el derecho a través del cual los ciudadanos pueden solicitar la modificación de aquella información falsa o inexacta sobre su persona.

Asimismo, la Ley Orgánica 2/1984, que en su artículo 1 dice que “Toda persona natural o jurídica tiene derecho a rectificar la información difundida por cualquier medio de comunicación social de hechos que le aludan, que considere inexactos y cuya divulgación pueda causarle perjuicio”.

La rectificación de datos personales inexactos o incompletos es también una obligación del Responsable del Tratamiento para garantizar el principio de exactitud de los datos, así como para garantizar la licitud del tratamiento.

A continuación, se facilita el formulario de solicitud de rectificación a los datos personales, así como un modelo con la posible respuesta del mismo, en los *Anexos Prácticos.*

DERECHO DE OPOSICIÓN

El Derecho de Oposición es aquel que permite a los interesados oponerse al tratamiento de sus datos personales. Se incluye en la lista de los Derechos ARSULIPO.

Se encuentra regulado en el artículo 21 del RGPD y en el 18 de la LOPDGDD. Se trata de un derecho independiente (sin necesidad de ejercerse otro derecho previa o posteriormente) y personalísimo (solo puede ejercerlo el propio interesado, representantes legales o herederos).

A continuación, se facilita el formulario de solicitud de oposición a los datos personales, así como un modelo con la posible respuesta del mismo, en los *Anexos Prácticos.*

DERECHO DE SUPRESIÓN

El Derecho de Supresión es aquel que permite a los interesados revocar su propio consentimiento prestado anteriormente. A través del ejercicio del mismo se exige la eliminación de cualquier dato personal mediante petición directa al Responsable del Tratamiento.

Se trata de uno de los derechos ARSULIPO, recogido tanto en el Reglamento Europeo de Protección de Datos como en la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Dentro de este derecho se incluye también el derecho “al olvido”, el cual es la manifestación del derecho de supresión aplicado de forma concreta a los buscadores de Internet. Se traduce en el derecho a impedir la divulgación de los datos personales o información a través de Internet siempre y cuando su publicación no encaje con los principios de adecuación y pertinencia previstos en la norma.

A continuación, se facilita el formulario de solicitud de supresión a los datos personales, así como un modelo con la posible respuesta del mismo, en los *Anexos Prácticos.*

DERECHO DE LIMITACIÓN

El derecho a la limitación del tratamiento permite al interesado, cuyos datos personales son objeto de tratamiento, solicitar al responsable del tratamiento que aplique medidas sobre estos datos para, entre otras cosas, evitar su modificación o, en su caso, su borrado o supresión.

Para ejercer el derecho a la limitación de tratamiento de los datos personales, será necesario que la lleve a cabo el propio interesado, puesto que se trata de un derecho personalísimo, o sus representantes legales o herederos.

A continuación, se facilita el formulario de solicitud de limitación a los datos personales, así como un modelo con la posible respuesta del mismo, en los *Anexos Prácticos.*

DERECHO A LA PORTABILIDAD

El derecho a la portabilidad de los datos consiste en otorgar a cualquier ciudadano europeo el derecho a que cualquier empresa que trate sus datos personales de forma automatizada se los ceda o los transfiera a cualquier otra empresa que este les indique en un formato estructurado, inteligible y automatizado.

Es decir, el ciudadano puede exigir a las empresas que estén tratando sus datos, incluso aquellas que manejan Big Data que se los devuelvan o que los pasen a otra empresa.

se aplica en todos los Estados miembros de la Unión Europea, bajo el amparo del RGPD o Reglamento General de Protección de Datos.

A continuación, se facilita el formulario de solicitud de portabilidad a los datos personales, así como un modelo con la posible respuesta del mismo, en los *Anexos Prácticos.*

DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS

Este derecho pretende garantizar que los interesados no sean objeto de una decisión basada únicamente en el tratamiento de sus datos, incluida la elaboración de perfiles, que produzcan efectos jurídicos sobre ellos o les afecte de forma significativa.

No obstante, este derecho no será aplicable cuando sea necesario para la celebración o ejecución de un contrato entre el interesado y el responsable de tratamiento, cuando el tratamiento de los datos se fundamente en el consentimiento prestado de forma previa o bien, cuando esté autorizado por el Derecho de la Unión o de los Estados miembros y se establezcan medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos del interesado.

A continuación, se facilita el formulario de solicitud de no ser objeto de decisiones individuales automatizadas en los *Anexos Prácticos.*

# Gestión de riesgo y evaluación de impacto

La gestión del riesgo es un elemento fundamental en los procesos de cualquier organización y es una parte inherente de la gestión de toda entidad, proyecto o actividad humana.

La gestión de riesgo está formada por un conjunto de acciones ordenadas y sistematizadas con el propósito de controlar las posibles consecuencias que una actividad puede tener sobre un conjunto de bienes o elementos que han de ser protegidos.

Precisa de un análisis, es decir, una reflexión crítica y objetiva de un tratamiento, requiere tomar decisiones que se han de plasmar en hechos concretos que minimicen el impacto sobre los activos hasta unos niveles tolerables. El RGPD demanda la identificación, evaluación y mitigación, realizadas de una forma objetiva, del riesgo para los derechos y libertades de las personas en los tratamientos de datos personales.

Por tanto, el RGPD establece la obligación de gestionar el riesgo que para los derechos y libertades de las personas supone un tratamiento.

El RGPD establece las obligaciones relativas a la evaluación de impacto relativa a la protección de datos (EIPD), fundamentalmente, en los artículos 35 y 36. Como establece el artículo 35:

Cuando sea probable que un tipo de tratamiento, …, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, …, una evaluación del impacto.

No es obligatorio que para cualquier tratamiento de datos personales sea necesario realizar una EIPD, pero sí que es obligatorio que se realice cuando hay una probabilidad de que entrañe un alto riesgo. La existencia de un grado razonable de presunción de que el tratamiento puede entrañar un alto riesgo hace imprescindible la realización de una EIPD. Podemos definir el EIPD como proceso que obliga a actuar, y de conformidad con lo previsto en el Reglamento, como un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos.

Por todo lo expuesto, se extrae que es necesario realizar una previa identificación de los factores de riesgo que puedan propiciar un evento capaz de ocasionar un impacto den los derechos y libertades de los interesados.

Para dar respuesta a esta necesidad, el RGPD impone al Responsable de la obligación de realizar una evaluación del nivel de riesgo respecto de los tratamientos que realiza, teniendo en cuenta todos los aspectos del tratamiento, que se derivan de la naturaleza, ámbito, contexto y fines del tratamiento.

Por consiguiente, y con el fin de cumplir con la obligación impuesta, elaboramos la propia evaluación de impacto a través del **Mapa de Riesgos** que se adjunta a la presente documentación, en el cual se prevén cada uno de los puntos de mayor riesgo de la organización y sobre los cuales se van a adoptar una serie de medidas adicionales de control, adecuación y prevención.

# Actuación en caso de brechas de seguridad

El RGPD define, de un modo amplio, las “brechas de datos personales” como:

Todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

No tendrán consideración de brecha de datos personales sujetas a los artículos 33 y 34 del RGPD aquellos incidentes que:

* No afecten a datos personales, es decir, a datos que no sean de personas físicas identificadas o identificables.
* No afecten a tratamientos de datos personales llevados a cabo por un responsable o un encargado.
* Ocurran en tratamientos llevados a cabo por una persona física en el ámbito doméstico.

Recae sobre el Responsable del Tratamiento la obligación de notificar tanto a la Autoridad de Control como a los interesados las posibles brechas de datos personales que puedan darse.

En primer lugar, respecto de la obligación de notificar a la Autoridad de Control, se establece en el artículo 33 del RGPD, que tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de datos personales debe efectuar la correspondiente notificación a la Autoridad de Control competente, cuando sea probable que la brecha constituya un riesgo para los derechos y libertades de las personas. En su caso, debe realizarse sin dilación y a más tardar en las 72 horas siguientes, computando también las horas trascurridas durante fines de semana y festivos.

El criterio para determinar si un incidente ha producido “una brecha de datos personales” se recoge en el propio RGPD: “toda violación de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.”

Con carácter general, en el ámbito privado, los responsables del tratamiento afectado por la brecha deberán notificar a la Agencia Española de Protección de Datos:

* Cuando su único establecimiento esté localizado en España.
* Si tienen varios establecimientos en la Unión Europea, únicamente cuando el establecimiento principal esté localizado en España.
* Si no tienen establecimiento principal en la Unión Europea, sólo en el caso de que hayan designado un representante en España.
* Si no tienen establecimiento ni representante en la Unión Europea, en el caso de que la brecha de datos personales cuente con afectados en España.

Los responsables de tratamiento con establecimiento principal en otro Estado Miembro de la Unión Europea, o que no tengan un establecimiento en la Unión, pero hayan nombrado un representante en otro Estado Miembro, deberán notificar a la Autoridad de Control de dicho Estado Miembro.

El artículo 33 del RGPD establece que la notificación de brechas de datos personales a la Autoridad de Control deberá como mínimo:

* “Describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;”
* “Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto del que pueda obtenerse más información;”
* “Describir las posibles consecuencias de la violación de la seguridad de los datos personales;”
* “Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.”

Por otro lado, también se prevé la obligación de notificar las brechas de seguridad a los interesados que hayan resultado afectados. Se trata de las personas físicas cuyos datos personales se han visto afectados por una brecha comprometiendo la confidencialidad, integridad y/o disponibilidad de esos datos, y quienes pueden sufrir las consecuencias.

El artículo 34 del RGPD establece que cuando sea probable que la brecha de datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable de tratamiento comunicará la brecha de datos personales a los afectados sin dilación indebida (en el RGPD no se establece un plazo concreto)

Por tanto, tan pronto como el responsable de tratamiento tenga constancia de la brecha de datos personales deberá valorar el riesgo para las personas afectadas y determinar la necesidad de comunicar la brecha a los afectados. En caso de que el riesgo se determine como alto, la comunicación a los afectados deberá realizarse a la mayor brevedad posible.

De conformidad con el artículo 34 del RGPD, la comunicación a las personas afectadas se realizará en un lenguaje claro y sencillo, con el siguiente contenido mínimo:

* Datos de contacto del Delegado de Protección de Datos, o en su caso, del punto de contacto en el que pueda obtenerse más información.
* Descripción general del incidente y momento en que se ha producido.
* Las posibles consecuencias de la brecha de datos personales.
* Descripción de los datos e información personal afectados.
* Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.
* Otras informaciones útiles a los afectados para que puedan proteger sus datos o prevenir posibles daños.

La comunicación preferentemente se deberá realizar de forma directa al afectado, ya sea por teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier otro medio dirigido al afectado que el responsable considere adecuado.

# Encargado de tratamiento de datos personales

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste.

El encargado puede realizar todos los tratamientos, automatizados o no, que el responsable del tratamiento le haya encomendado formalmente.

El responsable del tratamiento debe elegir un encargado del tratamiento que ofrezca garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD, y que garantice la protección de los derechos de las personas afectadas. Existe, por tanto, un deber de diligencia en la elección del responsable.

La regulación de la relación entre el responsable y el encargado del tratamiento debe establecerse a través de un contrato o de un acto jurídico similar que los vincule. El contrato o acto jurídico debe constar por escrito, inclusive en formato electrónico.

En el caso de designar un encargado de tratamiento, deberá formalizar el contrato vinculante de la relación. Disponen de un modelo en los *Anexos Prácticos.*

# Transferencias de datos personales con carácter internacional

Las transferencias internacionales de datos suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega).

Los datos solo podrán ser comunicados fuera del Espacio Económico Europeo:

* A países, territorios o sectores específicos (el RGPD incluye también organizaciones internacionales sobre los que la Comisión haya adoptado una decisión reconociendo que ofrecen un nivel de protección adecuado).

Se añade una excepción al listado que en su momento estableció la Directiva 95/46. Se trata de la posibilidad de que el responsable pueda transferir datos a un país sin nivel adecuado de protección cuando esa transferencia sea necesaria para satisfacer intereses legítimos imperiosos del responsable y la transferencia no es repetitiva y afecta sólo a un número limitado de interesados. En todo caso, la transferencia solo será posible si no prevalecen los derechos, libertades e intereses de los afectados y deberá comunicarse a la autoridad de protección de datos.

* Cuando se hayan ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino
* Cuando se aplique alguna de las excepciones que permiten transferir los datos sin garantías de protección adecuada por razones de necesidad vinculadas al propio interés del titular de los datos o a intereses generales.

A falta de decisión de adecuación y de garantías adecuadas únicamente se podrán realizar si se cumple alguna de las condiciones siguientes:

* La persona interesada haya dado explícitamente su consentimiento, después de haber sido informada de los posibles riesgos
* La transferencia sea necesaria para la ejecución de un contrato entre la persona interesada y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud de la persona interesada
* La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica
* La transferencia sea necesaria por razones importantes de interés público
* La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones
* La transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando la persona interesada esté física o jurídicamente incapacitada para dar su consentimiento
* La transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta

Si no resultase aplicable ninguna de estas excepciones, solo se podrá llevar a cabo una transferencia si no es repetitiva, afecta solo a un número limitado de personas interesadas, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades de la persona interesada, y el responsable del tratamiento evalué todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofrezca garantías apropiadas con respecto a la protección de datos personales.

En este supuesto el responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14 del RGPD, el responsable del tratamiento informará a la persona interesada de la transferencia y de los intereses legítimos imperiosos perseguidos.

Delegado de Protección de Datos Personales

El RGPD establece la figura del Delegado de Protección de Datos (DPD), que será obligatorio en:

* 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

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

Se permite nombrar un solo DPD para un grupo empresarial siempre que sea accesible desde cada establecimiento del grupo. La accesibilidad debe entenderse en un sentido amplio. Incluye la accesibilidad física para el propio personal del grupo y también la posibilidad de que los interesados contacten con el DPD en su lengua, aun cuando el DPD esté adscrito a un establecimiento en otro Estado Miembro.

La AEPD ha optado por promover un sistema de certificación de profesionales de protección de datos como herramienta útil a la hora de evaluar que los candidatos a ocupar el puesto de DPD reúnen las cualificaciones profesionales y los conocimientos requeridos. Las certificaciones serán otorgadas por entidades certificadoras debidamente acreditadas por la Entidad Nacional de Acreditación, siguiendo criterios de acreditación y certificación elaborados por la AEPD en colaboración con los sectores afectados.

La certificación no será un requisito indispensable para el acceso a la profesión, será sólo una opción a disposición de responsables y encargados para facilitar su selección de los profesionales llamados a ocupar el puesto de DPD. Pero responsables y encargados pueden tomar en consideración otras cuestiones u otros medios para demostrar la competencia de los DPD.

Se permite que el DPD mantenga con responsables o encargados una relación laboral o mediante un contrato de servicios. Es decir, permite que pueda contratarse el servicio de DPD con personas físicas o jurídicas ajenas a la organización.

Está permitido que el DPD desarrolle sus funciones a tiempo completo o parcial. En este último caso, es preciso evitar que existan conflictos de intereses. Estos conflictos pueden surgir cuando el DPD, en su tarea de supervisión de las actividades de tratamiento de datos llevadas a cabo por la organización, debe valorar su propio trabajo dentro de ella, como sucede si se designa DPD al responsable de tecnologías de la información (cuando estas tecnologías se emplean para el tratamiento de datos) o al responsable de un área de negocio que decide sobre determinados tratamientos.