Colegio Oficial de Psicólogos de Madrid

Protección de datos en Psicología: Guía práctica

Adaptación al Reglamento General Europeo de Protección de Datos

www.copmadrid.org

Colegio Oficial de Psicólogos de Madrid
Cuesta de San Vicente, 4, 5º. 28008 Madrid
formacion.online@cop.es

Depósito Legal:

Nota aclaratoria: En beneficio de una mayor facilidad y claridad en la lectura y comprensión del texto, se utilizará un lenguaje igualitario y no sexista. No obstante, se explicita que, en el uso de términos como los profesionales, los estudiantes, los responsables, los psicólogos,... y cualquier otro que se encuentre en este documento, se hace referencia a hombres y mujeres, e incluye el masculino y el femenino.

1. Índice

1. ¿Qué es el Reglamento General Europeo de Protección de Datos?

El **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016** (Reglamento General de Protección de Datos o RGPD) 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 **se debe empezar a aplicar partir de mayo de 2018.**

El RGPD trata de homogeneizar la normativa de protección de datos para todos los estados miembros de la Unión Europea. Al ser un Reglamento, es una norma de efecto directo que no requiere transposición a la legislación de cada estado, es decir, es de **aplicación directa**, pero que sí ofrece a los estados miembros cierta flexibilidad en algunos aspectos, como por ejemplo elegir la edad de consentimiento de los menores de edad, que queda abierta a los estados para decidir dentro del margen de 13 a 16 años o determinar quién está obligado a disponer de un Delegado de Protección de Datos DPD/DPO. Es por eso que la legislación española también va a cambiar para determinar los matices que considere oportunos.

El 24 de noviembre de 2017, el Congreso de los Diputados remitió a las Cortes Generales el **21/000013 Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal (PLOPD)** que sustituirá a la actual LOPD, y que se prevé que entrará en vigor en **mayo de 2018** a la vez que el RGPD. Por ello, algunos aspectos están ya claros, pero otros dependerán de lo que indique la nueva legislación española.

En este **periodo transitorio** hasta mayo de 2018, hay que ir adaptándose y adoptando las medidas pertinentes para poder cumplir con la nueva legislación, sin dejar de cumplir la legislación actual, ya que seguirá vigente hasta esa fecha.

La Agencia Española de Protección de Datos ha creado un apartado donde reúne toda la información sobre el RGPD, y al que se puede acceder desde este **enlace**.

Desde el Colegio Oficial de Psicólogos de Madrid os mantendremos informados de cualquier cambio que se produzca hasta esa fecha.

2. ¿Qué cambios implica?

Los **principios y conceptos del RGPD** son en realidad muy parecidos a los de la anterior directiva y a los de la LOPD y el Real Decreto de aplicación de la LOPD (RDLOPD), por lo que si como Responsables del Tratamiento se está cumpliendo actualmente con la legislación vigente, se parte de una muy buena base para adaptarse al RGPD.

A. Principios de Protección de Datos

Los principios generales que rigen a la hora de interpretar y aplicar el RGPD son básicamente los mismos que en la LOPD y el RDLOPD (y que aparecen en la Guía de protección de datos personales en psicología: implicaciones y buenas prácticas) con alguna novedad, eso sí. Además varía la forma de nombrarlos o el encuadre que tienen en el Reglamento, y generan nuevas obligaciones, pero se refieren a lo mismo. Por ejemplo el "*Principio de calidad*" que se explica en la mencionada guía, en el nuevo Reglamento se desglosa en varios, el de *licitud, limitación de la finalidad, minimización, exactitud, limitación del plazo de conservación;* o el principio de *"Derecho de información",* ahora se incluye en el de *transparencia,* pero básicamente son los mismos conceptos que ya hemos visto.

A continuación podemos ver los Principios de protección de datos según el Reglamento General de Protección de Datos.

1. Principio de responsabilidad proactiva/Enfoque de riesgos
2. Principio de lealtad
3. Principio de transparencia o información
4. Principio de licitud y consentimiento
5. Principio de limitación de la finalidad en la recogida de datos
6. Principio de minimización
7. Principio de exactitud
8. Principio de limitación del plazo de conservación
9. Principio de seguridad de la información

No nos vamos a detener en todos los principios, puesto que se trata básicamente de lo que aparece en la Guía, pero sí vamos a ver con más detalle alguno por ser novedoso. En el siguiente apartado veremos las nuevas obligaciones que surgen de estos principios con la nueva legislación.

Dos conceptos nuevos que constituyen la **mayor innovación** del nuevo Reglamento Europeo, y que suponen un cambio importante en la forma de afrontar la protección de datos.

- El principio de responsabilidad proactiva
- El enfoque de riesgos

La Guía del Reglamento de Protección de Datos para Responsables de tratamiento editada por la Agencia de Protección de Datos ofrece estas definiciones de estos conceptos.

Principio de responsabilidad activa	Enfoque de riesgos
El RGPD describe este principio como 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, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben **determinar de forma explícita la forma en que 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.	El RGPD señala que las 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.

Otros cambios importantes son:

Tratamiento de datos de menores

El RGPD establece nuevas pautas para el tratamiento de datos de menores de edad, por ejemplo en el ámbito de los servicios de la sociedad de la información, como es el caso de las **redes sociales**, será legal el tratamiento siempre y cuando tengan más de **16 años**, pero permite a los estados miembros rebajar esa edad hasta los 13 años, en **el caso de España el proyecto de ley indica que se rebajará de los 14 años actuales a los 13 años**. Por debajo de esa edad se deberá solicitar consentimiento, que deberá ser verificable, se debe así mismo habilitar medios para verificar la edad del menor.

En el caso de los menores es particularmente importante que la información que se le facilite sea **claramente comprensible** para el menor.

Régimen sancionador

Las sanciones se incrementan de forma importante:

LOPD / RDLOPD	RGPD
▪ Entre 401,01 € y 60.101,21 € ▪ Entre 40.101,21 € y 300.00 € ▪ Entre 300.000€ y 601.012,01€ (Tras la modificación de la Ley de Economía Sostenible)	▪ No se hace mención a sanciones mínimas. ▪ Hasta 10.000.000€ o 2% como máximo del volumen de negocio anual global del ejercicio anterior (lo que resulte de mayor cuantía). ▪ Hasta 20.000.000€ o 4% como máximo del volumen de negocio anual global del ejercicio (lo que resulte de mayor cuantía).

El proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, (actualmente en las Cortes Generales) divide las **infracciones** en leves, graves y muy graves (se pueden consultar en los artículos 71-74 del proyecto de Ley).

El proyecto indica que:

> "Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo. 2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta: a) El carácter continuado de la infracción. b) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal. c) Los beneficios obtenidos como consecuencia de la comisión de la infracción. d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción. e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente."

Para más información sobre las el régimen sancionador se puede consultar el **RGPD** y lo relacionado con el proyecto de ley, en el siguiente **enlace**.

Como veis, ahora tenemos una mayor responsabilidad y requiere **no sólo cumplir con las obligaciones y medidas de seguridad** que nos indicaba el RD LOPD según el nivel de seguridad del fichero, sino que hay que **poder acreditar que se ha hecho todo lo posible para garantizar la seguridad del tratamiento**.

Luego veremos con más detenimiento cómo hacerlo, ahora vamos a ver las nuevas obligaciones con el **RGPD**

B. Principales obligaciones

En el cuadro comparamos las obligaciones que tenemos con la LOPD y las que tendremos con la nueva legislación

LOPD / RDLOPD	RGPD
▪ Inscripción de ficheros en la AEPD ▪ Deber de información ▪ Consentimiento para el tratamiento ▪ Contratos con terceros (encargados de tratamiento) ▪ Documento de seguridad e implantación de medidas de seguridad ▪ Facilitar derechos ARCO ▪ Auditoría bienal (nivel medio y alto)	▪ No inscripción de ficheros en AEPD, pero sí Inventario y registro de actividades de tratamiento ▪ Cambios en el deber de información, más aspectos a informar y formato en capas. ▪ Cambios en el deber de informar en los contratos con terceros y la responsabilidad de los encargados, garantizar la adecuación del encargado ▪ Nuevas formas de licitud del tratamiento ▪ Responsabilidad Proactiva: ✓ Privacidad desde el diseño y por defecto ✓ Análisis de riesgo y evaluaciones de impacto. ✓ Documentar medidas de seguridad ✓ Notificación de violaciones de seguridad a AEPD e interesados ✓ Delegado de protección de datos DPO/DPD ▪ ARCO más nuevos derechos, (limitación del tratamiento, portabilidad de los datos y derecho al olvido ▪ No auditoría bienal, pero sí cuando determine el responsable para garantizar seguridad.

3. ¿Entonces qué tengo que hacer?

A. Lista de verificación

Para que nos sirva de guía para repasar todos los cambios vamos a utilizar la lista de verificación que ofrece la Agencia Española de Protección de Datos en la Guía del Reglamento de Protección de Datos para Responsables de tratamiento, combinándolo con los cambios que hemos comentado en el apartado anterior.

Vamos a ir viendo **paso a paso** qué preguntas tenemos que hacernos para verificar si el tratamiento que ya estamos realizando se ajusta a lo que nos demanda el RGPD o si tenemos que realizar algún cambio y cómo hacerlo.

Inventario y registro de tratamiento

El primer paso será hacer un **inventario de los tratamientos de datos personales** que se realizan para **identificar las áreas de riesgo**, esto es, saber qué datos estamos tratando y cómo los estamos tratando y todos los riesgos que pueden afectar a la seguridad de los datos, para poder aplicar las medidas que les correspondan, las más adecuadas para nuestro tratamiento en concreto. Ya no nos sirve como con la legislación actual de protección de datos, únicamente aplicar las medidas de seguridad según el nivel de seguridad determinado por el tipo de datos (básico, medio y alto), según lo indicado por la LOPD y su reglamento de desarrollo, ahora somos nosotros los que determinamos **qué medidas son las más adecuadas** valorando todo lo relacionado con el tratamiento que hacemos. Nuestra responsabilidad será decidir, tras analizar todos los posibles riesgos, qué haremos para proteger el tratamiento y por supuesto tenemos que **poder acreditarlo ante la Agencia Española de Protección de Datos**, documentándolo.

Para realizar este inventario de tratamientos, si ya hemos inscrito nuestros ficheros, podemos utilizar la herramienta propuesta por la Agencia de Protección de Datos para facilitar la labor de los responsables de tratamiento, y **solicitar una copia de la información que facilitamos en su momento al inscribir los ficheros.** Esta información puede guiar la realización del inventario de tratamiento, y ayudarnos en el análisis de riesgos.

Podemos acceder a dicha herramienta desde este enlace. Si tenemos certificado electrónico nos facilitarán la información en formato electrónico (XML o Excel), si no lo tenemos nos pueden facilitar la información por correo postal.

El reglamento se centra más en las **actividades de tratamiento** que realizamos que en los ficheros. Estas **actividades de tratamiento** podrían asimilarse a lo que, con la actual legislación, llamamos **finalidades del fichero**. Antes notificábamos un fichero y explicábamos las finalidades para las que recogíamos los datos, con el nuevo reglamento el foco se pone en las actividades de tratamiento.

Con esa información y detallando todas las operaciones que se realizan sobre cada conjunto estructurado de datos podríamos empezar a elaborar el **inventario**.

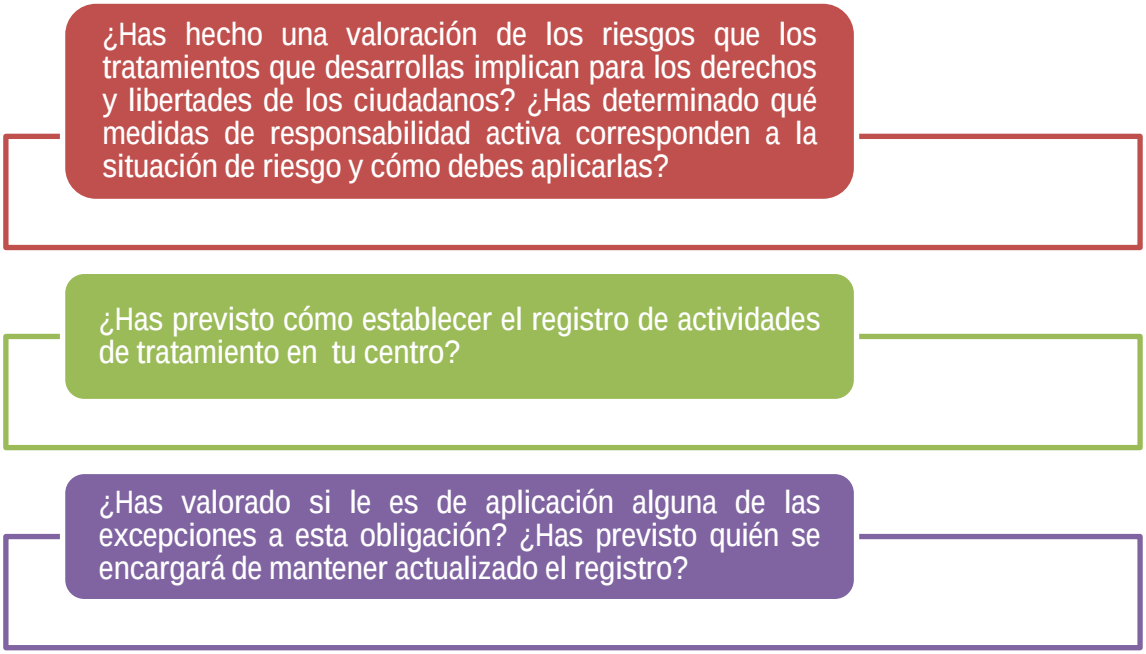
Si no hemos realizado ya la inscripción y por tanto no podemos descargar esa información, la *Guía del Reglamento de Protección de Datos para Responsables de tratamiento* propone para guiarnos, partir pensando las operaciones de tratamiento concretas vinculadas a una finalidad básica común de todas ellas (por ejemplo, "gestión de clientes", "gestión contable" o "gestión de recursos humanos y nóminas") o con arreglo a otros criterios distintos.

En este registro de actividades **el responsable debe** como mínimo:

- Describir qué datos recoge
- Con qué fin se tratan
- A quién o quiénes los comunica
- Si los transfiere a terceros países
- Qué medidas técnicas y organizativas aplica para preservar su seguridad, y cuándo podrá suprimirlos.
- En su caso, los datos de contacto del delegado de protección de datos

Para tratamientos muy sencillos, de escaso riesgo, que no implican datos sensibles como los de salud, se puede utilizarla la herramienta Facilita, pero en nuestro caso lo normal es que tengamos que hacer un análisis de riesgos, y por tanto no nos serviría esta aplicación. La Agencia pretende modificar la herramienta Facilita para que se pueda utilizar en casos más complejos que impliquen datos sensibles, pero de momento no puede utilizarse.

Las preguntas pertinentes en este momento son las siguientes



Nuevas formas de licitud del tratamiento

Al ver las obligaciones, conocimos que el RGPD contempla otras bases legales para tratar con datos de carácter personal distintas al consentimiento del interesado. Las bases legítimas son las siguientes.

- 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.

Hay que pensar por tanto cuál de ellas se adapta mejor al tipo de tratamientos que llevamos a cabo. Hay que tener en cuenta que aunque no se necesite consentimiento si por ejemplo la base jurídica es una relación contractual en la que es necesario tratar datos para prestar el servicio que ofrezcamos, **no dejamos de tener la obligación de informar, y de dejar constancia de haber realizado dicha comunicación.**

En el caso del **consentimiento** tiene que ser "**inequívoco**". Esto quiere decir que debe realizarse a través de una **manifestación del interesado o mediante una clara acción afirmativa**. A diferencia del Reglamento de Desarrollo de la LOPD, n**o se admiten formas de consentimiento tácito o por omisión**, ya que se basan en la inacción.

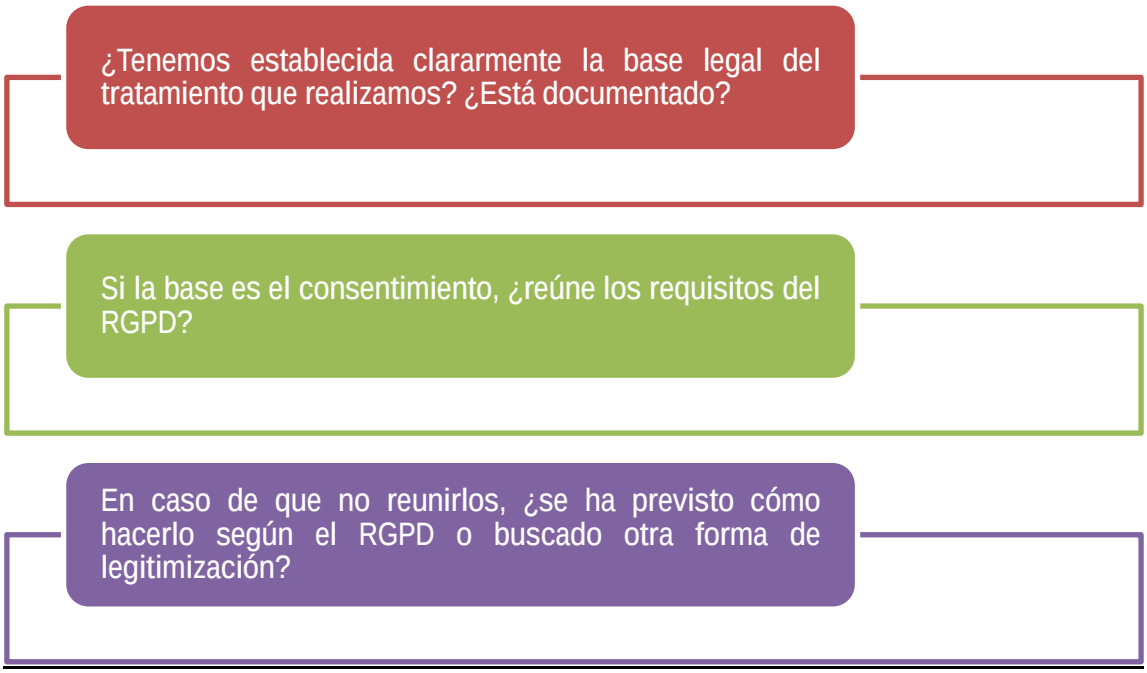
En algunos casos, como cuando el responsable trata los datos para elaborar perfiles, si trata datos sensibles o si realiza transferencias internacionales de datos, debe de ser además **explícito**.

El Considerando 32 del RGPD dice lo siguiente:

> "El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.":

Si has estado recogiendo el consentimiento de esta forma, no hará falta hacer nada. Si no es así, habría que solicitarlo o buscar otra fuente de legitimación para tratar los datos.

En este momento debemos hacernos las siguientes preguntas



Cambios en la forma de informar

En la Guía de protección de datos personales en psicología: implicaciones y buenas prácticas) se indica que hasta ahora, como responsable de fichero, **se debe informar** sobre los siguientes aspectos:

- Nombre del fichero.
- Responsable del fichero.
- Finalidad de la recogida de los datos.
- Posibles cesiones.
- Información relativa a la forma de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- Aclarar qué información será imprescindible ofrecer para continuar el proceso y cuál será opcional. La persona debe conocer en todo momento qué consecuencias tendrá la información que facilita.

El nuevo Reglamento europeo (RGPD) añade **requisitos adicionales** en cuanto a la necesidad de informar:

- La base jurídica o legítima o legitimación del tratamiento.
- El plazo o criterios de conservación de la información.
- La existencia de decisiones automatizadas o elaboración de perfiles
- La previsión de transferencias a Terceros Países.
- El derecho a presentar una reclamación ante las Autoridades de control.

- Los datos de contacto del Delegado de Protección de Datos.

Si los datos no se obtienen directamente del propio interesado, habrá que informar de:

- El origen de los datos.
- La categoría de los datos.

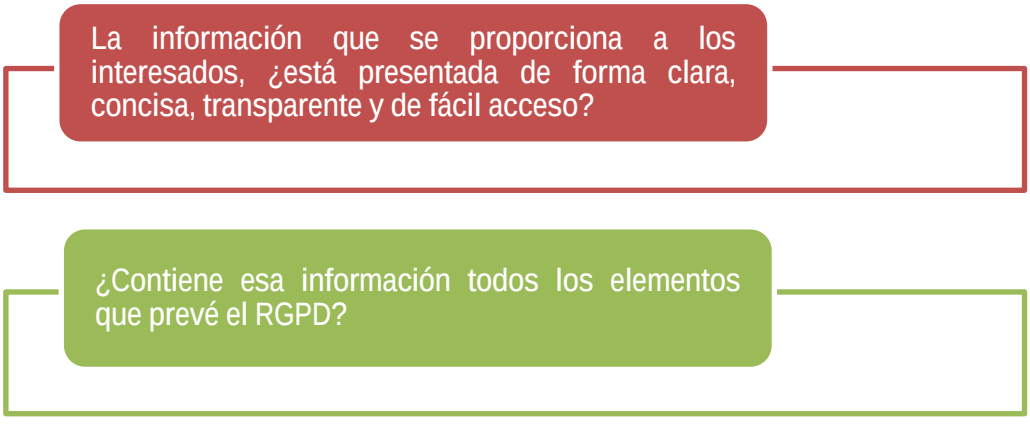
Al ser el responsable del fichero el que debe probar que ha cumplido con el deber información, es necesario **conservar el soporte que acredite su cumplimiento** durante el tiempo que persista el tratamiento de los datos.

El RGPD da **importancia a la forma de comunicar la información**, nos dice que debe facilitarse la información con un lenguaje claro y sencillo, de forma concisa, transparente, inteligible y de fácil acceso, nada de fórmulas farragosas de difícil interpretación.

Las Autoridades de protección de datos proponen que se utilice un **formato de dos capas**, una primera capa con la **información básica** y otra en la que **ampliamos la información**. Proponen que se presente la información en formato de **tabla**, similar a la utilizada para presentar la información nutricional de los alimentos.

La Agencia Española de Protección de Datos ha elaborado una **Guía** para facilitar los cambios que supone el nuevo reglamento, y en la que se puede ver de forma detallada toda la información que hay que facilitar a los usuarios.

Las cuestiones que hay que plantearse en relación a este aspecto son los siguientes:



Cambios en la facilitación de derechos

En relación a los derechos a facilitar a los clientes/pacientes nos encontramos las siguientes **novedades**:

- La obligación de articular procedimientos que faciliten a los interesados ejercitar sus derechos por medios electrónicos y que puedan acreditar su ejercicio por el mismo medio.
- En caso de considerar que la solicitud de alguno de los derechos es infundado o excesivo, es el responsable el que debe demostrarlo si pretende que tenga un coste para el interesado para compensar los gastos que suponga al responsable facilitar el derecho. El importe que se cobre no puede implicar un ingreso adicional, pero si puede ser el importe del *verdadero coste de la tramitación de la solicitud.*
- Se debe contestar en el plazo de un mes. Se podría ampliar a dos meses cuando la solicitud sea especialmente compleja, y en ese caso se comunicará este aspecto dentro del primer mes. Antes había diferentes plazos según el derecho que se ejerciera, ahora es el mimo plazo (un mes para todos los derechos).
- Si se decide que no se va a atender a la solicitud, se deberá informar y motivar su negativa dentro del plazo de un mes.
- Se reconoce el derecho a obtener una copia de los datos personales objeto del tratamiento en todos los casos. En el caso de la historia clínica ya era así también con la anterior legislación.
- Los derechos se podrán atender facilitando el acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales.
- Se deben tomar las medidas oportunas para la identidad de quienes soliciten acceso y de quienes ejerzan los restantes derechos ARCO.
- Da la posibilidad al responsable que trate una gran cantidad de información sobre un interesado que se le especifique la información a que se refiere su solicitud de acceso.
- También da la posibilidad de contar con la colaboración de los encargados de tratamiento para atender al ejercicio de derechos de los interesados, eso sí deberá incluirse este aspecto en el contrato de encargo de tratamiento.

Además los **derechos ARCO** se han ampliado, pasan a ser los siguientes:

- El derecho de acceso
- El derecho de rectificación

- El derecho a supresión ampliado (en el contexto de internet sería el derecho al olvido)
- El derecho a la limitación del tratamiento
- El derecho a la portabilidad de datos
- El derecho de oposición (derecho a la exclusión voluntaria, por ejemplo oposición a que se usen con fines de prospección comercial o investigación o fines estadísticos)
- El derecho a no someterse a la toma de decisiones automatizadas, incluyendo la elaboración de perfiles.

Vamos a ver con más detalle en qué consisten algunos de estos nuevos derechos, o mejor dicho la ampliación de estos derechos:

- **Derecho al olvido.** El derecho al olvido, es nuestro derecho a impedir que se difunda información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia. Por ejemplo cuando una información ya está obsoleta se tiene el derecho a limitar la difusión universal e indiscriminada de esa información, de esos datos personales en los buscadores, incluso cuando en su momento la publicación original fuera legítima, como es el caso de datos publicados en boletines oficiales o informaciones de periódicos amparadas por las libertades de expresión o de información.

  Es una consecuencia de la aplicación del derecho de cancelación de la información, pero en internet, obliga además a los responsables que hayan hecho públicos los datos personales en internet a borrar la información y a adoptar medidas técnicas para informar a otros responsables de la solicitud del interesado de borrar su información personal.

  En este enlace se puede acceder a más información sobre el derecho al olvido.

- **Derecho a la limitación del tratamiento**. Se refiere a que, a petición del interesado, no se apliquen a los datos que ha facilitado alguna de las operaciones de tratamiento que principio correspondan, por ejemplo si se solicita ejercer el derecho de rectificación o de oposición y el responsable todavía no ha contestado, podemos solicitar que mientras no se decida, no se utilicen los datos para nada.

Según la Guía del Reglamento de Protección de Datos para Responsables de tratamiento, los casos en los que se puede solicitar el ejercicio de este derecho son los siguientes:

- ✓ Cuando el tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello.
- ✓ El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender a la solicitud.
- ✓ 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.

- **Derecho a la portabilidad de los datos.** Es el derecho que puede ejercer un usuario, a solicitar una copia de todos los datos que se hayan facilitado. Esta copia se debe proporcionar al interesado en un formato estructurado, de uso común y lectura mecánica.

  El objeto es facilitar el traspaso de todos los datos de una persona de un responsable de tratamiento a otro, sería por ejemplo el caso de solicitar todos nuestros datos a una compañía telefónica para facilitárselos a otra compañía con la que vamos a contratar el servicio de telefonía. A no ser que no sea posible, los datos se traspasarán directamente de un responsable a otro, sin necesidad de que pasen por el propio interesado.

  Este derecho sólo puede ejercerse en estas circunstancias:

  - ✓ Cuando el tratamiento se efectúe por medios automatizados.
  - ✓ Cuando se base en el consentimiento o en un contrato.
  - ✓ Cuando se solicita en relación a datos que se haya proporcionado al responsable y que le conciernan, incluidos los datos derivados de la propia actividad del interesado.

En este enlace se puede ampliar información sobre el derecho a la portabilidad de los datos y en este otro podéis encontrar preguntas frecuentes sobre el tema.

En relación a los derechos ARCO habrá que revisar los siguientes aspectos:

- ¿Dispones de mecanismos para el ejercicio de derechos visibles, accesibles y sencillos?
- ¿Tienes establecidos procedimientos o mecanismos que te permitan verificar la identidad de quienes solicitan acceso o ejercen los demás derechos ARCO?
- ¿Pueden ejercerse los derechos por vía electrónica?
- ¿Tienes establecidos procedimientos que permitan responder a los ejercicios de derechos en los plazos previstos por el RGPD?
- ¿Has valorado si sería necesaria la colaboración de los encargados para responder a las solicitudes de los interesados y, si es así, tienes previsto incluir esta colaboración en los contratos de encargo?
- ¿Tienes previstos mecanismos para atender a posibles ejercicios del derecho a la limitación del tratamiento, de forma que los datos afectados puedan ser conservados sin ser objeto de las operaciones de tratamiento que corresponderían?
- ¿Has valorado si los tratamientos de datos que realizas pueden ser objeto del derecho a la portabilidad? En caso afirmativo ¿has previsto procedimientos o mecanismos para poder atender a este derecho y proporcionar los datos al interesado (o a otro responsable) en un formato estructurado, de uso común y susceptible de lectura mecánica?

Relaciones responsable-encargado del tratamiento

Otro de los aspectos que cambian son los relacionados con la relación entre el responsable y el encargado de tratamiento.

Uno de los cambios es la obligación de los responsables de **seleccionar un encargado de tratamiento** que nos ofrezca garantías de que van aplicar las medidas técnicas y organizativas apropiadas para que el tratamiento que realicen en nuestro nombre sea conforme con los requisitos del Reglamento.

Para seleccionar el responsable más adecuado, los responsables pueden valorar que los encargados estén **adheridos a códigos de conducta** o **certificados en el marco de los esquemas de certificación previstos por el RGPD**, lo que puede mostrar a las autoridades de control que estamos haciendo todo lo posible para garantizar un tratamiento seguro de los datos.

Además los encargados van a tener en algunos aspectos obligaciones propias que van más allá de las que tienen en el ámbito que los une al responsable y que pueden ser supervisadas separadamente por las autoridades de protección de datos.

Algunas de estas obligaciones son:

- Mantenimiento un registro de actividades de tratamiento.
- Determinar las medidas de seguridad más adecuadas aplicables a los tratamientos que realizan.
- Asignar un Delegado de Protección de Datos en los casos previstos por el RGPD.

Las relaciones entre el responsable y el encargado tienen que basarse en un **contrato o en un acto jurídico** que vincule al encargado respecto al responsable.

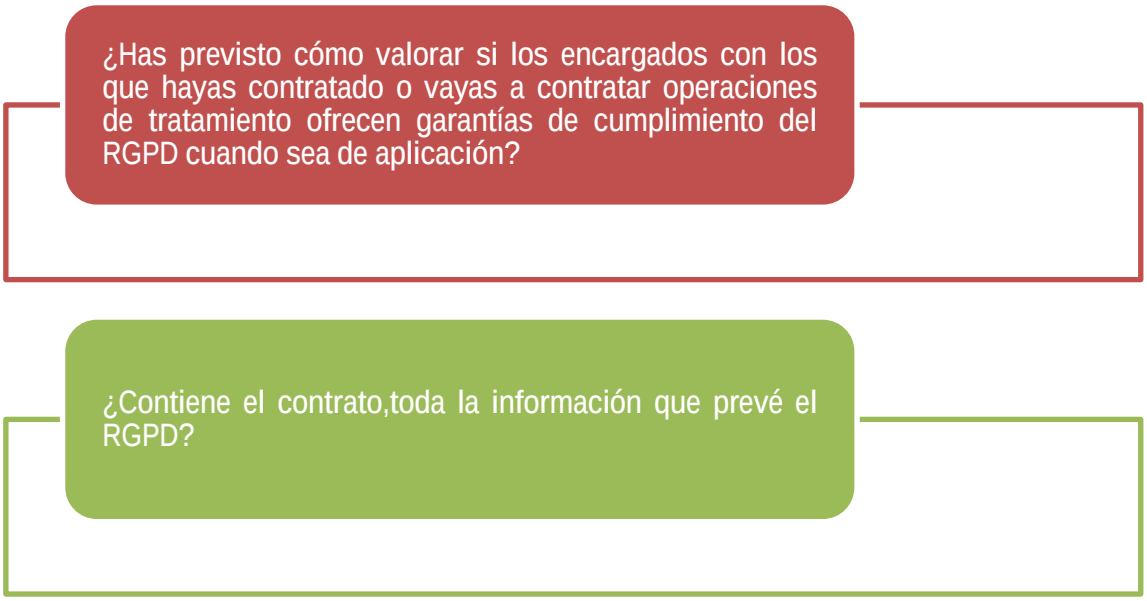
En el contrato debe incluirse información sobre lo siguiente:

- El objeto, duración, naturaleza y la finalidad del tratamientos
- El tipo de datos personales
- El tipo de categorías de interesados
- La obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable
- Condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones
- Puede asistir al responsable en la atención al ejercicio de derechos de los interesados, si así se le encarga.

Es importante saber que **los contratos de encargo** concluidos con anterioridad a la aplicación del RGPD en mayo de 2018 **deben modificarse y adaptarse** a estos requisitos.

En este enlace se puede consultar más información sobre la nueva relación encargado-responsable.

A continuación podemos ver algunas de las preguntas que nos tenemos que hacer en relación al encargado de tratamiento.



Protección de Datos desde el Diseño y por Defecto

A continuación vamos a ver otras cuestiones a tener en cuenta en relación a la responsabilidad proactiva, desde el diseño y por defecto.

Las medidas de seguridad se deben aplicar por el responsable con anterioridad a iniciar el tratamiento de datos, se debe empezar a pensar en todo lo relacionado con la protección de datos desde que se empieza un proyecto, desde que se diseña, y durante su desarrollo siempre que implique un tratamiento de datos de carácter personal.

B. Análisis de riesgo y evaluación de Impacto

Al principio del este anexo hablábamos de que el RGPD condiciona la adopción de medidas de seguridad, no en función del nivel de seguridad como hasta ahora indicaba la legislación actual, sino **en función del riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados**.

Hay que aplicar las medidas que después de evaluar los riesgos, nos garanticen que los tratamientos van a ser conformes a lo indicado por el reglamento y poder demostrarlo.

El RGPD determina que algunas medidas de seguridad, como la **evaluación de impacto**, por ejemplo, solo habrá que aplicarlas cuando tras un análisis de riesgos se determina que el tratamiento puede suponer un alto riesgo para los derechos y libertades de las personas. En otros casos las medidas se podrán modular según el tipo de riesgo y el nivel de riesgo que conlleve.

Por tanto es **obligatorio realizar una valoración del riesgo de los tratamientos** que realicen, para poder saber qué medidas hay que aplicar:

El tipo de análisis a realizar dependerá de los tipos, cantidad y variedad de tratamientos que se realicen, de la naturaleza de los datos, del número de interesados que pueden estar afectados.

No es lo mismo una gran organización que requiera por la complejidad del tratamiento que realice utilizar alguna de las metodologías de análisis existentes, como puede ser MAGERIT, que una empresa pequeña con tratamientos poco complejos que podrá realizar una análisis de riesgo sencillo, documentando lo básico, que puede consistir en pararse a pensar en el tratamiento. En esos casos puede ayudar la herramienta que ofrece la Agencia en su página para tratamientos de poco riesgo, Facilita.

Habría que reflexionar sobre aspectos como si se trata con datos sensibles, si se tratan datos de muchas personas, si se elaboran perfiles de personalidad, si se cruzan datos con otras fuentes, etc. Si tras reflexionar, se determinar que no se realizan tratamientos con un elevado riesgo, no deberá aplicar las medidas previstas en esos casos como es la evaluación de impacto.

En este enlace podéis ampliar información sobre análisis de riesgos.

¿Cuándo hay que realizar una evaluación de impacto?

Se debe 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.

Estos son los supuestos que se puede considerar como tratamientos de alto riesgo:

- Elaboración de perfiles sobre cuya base se tomen decisiones que produzcan **efectos jurídicos** sobre los interesados o que **les afecten significativamente** de modo similar
- **Tratamientos a gran escala de datos sensibles** (datos que releven opiniones políticas, creencias religiosas, los relativos a salud o la vida sexual, datos biométricos y genéticos)
- **Observación sistemática a gran escala** de una zona de acceso público
- O siempre que se consideré que puede resultar un tratamiento de alto riesgo.

Para valorar si un tratamiento se realiza a gran escala debe tenerse en cuenta (según el Grupo del Artículo 29, en su designación de Delegados de Protección de Datos):

- El número de interesados afectados, bien en términos absolutos, bien como proporción de una determinada población
- El volumen de datos y la variedad de datos tratados
- La duración o permanencia de la actividad de tratamiento
- La extensión geográfica de la actividad de tratamiento

Si se valora que el riesgo del tratamiento no va a poder mitigarse por medios razonables en términos de tecnología disponible y costes de aplicación, el responsable puede consultar con la Agencia.

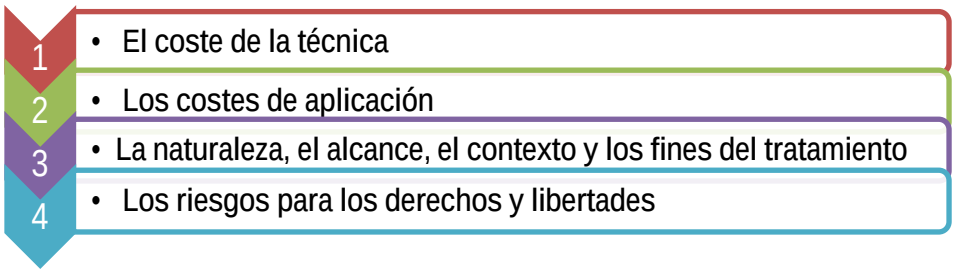
Para más información sobre **evaluaciones de impacto** se puede consultar la siguiente **Guía** editada por la Agencia Española de Protección de Datos.

Está previsto que la Agencia pueda elaborar listas de tratamientos en los que no se precisa evaluación de impacto.

Medidas de seguridad

En cuanto a las medidas de seguridad tanto técnicas como organizativas a implementar, habrá que decidirlas en función del nivel de seguridad que determinemos según los riesgos detectados en el análisis previo, que concluya que las medidas son realmente las más adecuadas para ofrecer un nivel de seguridad adecuado.

Las medidas técnicas y organizativas deberán establecerse teniendo en cuenta:



En muchos casos vamos a tener que seguir aplicando las mismas medidas que indicaba el anterior Reglamento de protección de datos, puesto que coincidirá el nivel asignado con el anterior criterio marcado por la ley (básico, medio, alto), pero puede ser que tras realizar el análisis de riesgos, determinemos que es necesario completarlas con medidas adicionales, incluso podría darse el caso de poder prescindir de alguna.

Notificación de violaciones de seguridad de los datos

Cuando se produzca una violación o quiebra de la seguridad de los datos, el responsable tendrá que **notificarla a la autoridad de protección de datos competente**, a menos que se valore como improbable que dicha quiebra de la seguridad suponga un riesgo para los derechos y libertades de las personas afectadas y deberá realizarse a ser posible, dentro de las **72 horas siguientes** a que el responsable tenga constancia de ella y por supuesto se deberá dejar debidamente documentada en un registro interno.

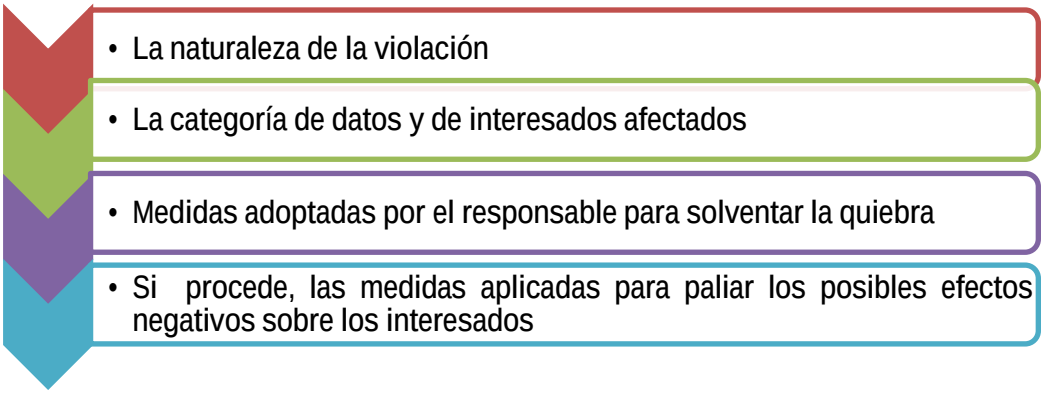
Si la situación fuera muy compleja y no se pudiera hacer en 72 horas, se podrá hacer de forma escalonada según se vaya teniendo más información; eso sí, si se retrasa habrá que explicar el motivo que ha ocasionado el retraso.

La Guía del Reglamento de Protección de Datos para Responsables de tratamiento explica así una violación de seguridad

Violación o quiebra de seguridad

El RGPD define las violaciones de seguridad de los datos, más comúnmente conocidas como "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 autorizados a dichos datos. Sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del RGPD y deben ser tratadas como el Reglamento establece.

Cualquier incidente no es una violación de seguridad, hay que tener certeza de que se ha producido y tener conocimiento suficiente de su naturaleza y alcance antes de comunicarla a la Agencia. La mera sospecha de que ha existido una quiebra o saber que ha habido algún tipo de incidente sin más, no deberían dar lugar, todavía, a la notificación, dado que en esas condiciones aún no sabemos si hay un riesgo para los derechos y libertades de los interesados. La notificación de contener como mínimo:



Si se valora que la quiebra de seguridad es tal que hay un alto riesgo para los derechos y libertades de las personas, **habrá que comunicárselo también a los afectados**, con el objetivo de que el afectado pueda reaccionar tan pronto como pueda, por ejemplo cambiando sus contraseñas.

Se considera que hay un alto riesgo de que la violación de seguridad ocasione daños importantes a los interesados cuando por ejemplo se desvele información confidencial, como contraseñas o participación en determinadas actividades o se difundan de forma masiva datos sensibles o se puedan producir perjuicios económicos para los afectados.

Puede ser que la misma Agencia tras conocer la violación de seguridad, se ponga en contacto con el responsable para indicarle que comunique la quiebra de seguridad a los afectados.

No será necesario notificar a los interesados cuando:

- Se hayan tomado con anterioridad a la quiebra de seguridad medidas técnicas u organizativas que hagan ininteligibles los datos a terceros, por ejemplo cuando se hayan encriptado los datos.
- Cuando con posterioridad a la quiebra se aplican medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice.
- Si la notificación supone un esfuerzo desproporcionado, en ese caso se podría sustituir por una comunicación pública.

La Agencia habilitará un canal para realizar las notificaciones de violaciones de seguridad.

Delegado de Protección de Datos (DPD)

Delegado de protección de datos
Es una figura encargada de orientar, asesorar, así como supervisar al responsable de actividades de tratamiento sobre el cumplimiento del RGPD, también realizará labores de mediación entre los usuarios y el responsable y será la persona de contacto con las Autoridades de control, podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

El RGPD establece como obligatoria la figura del **Delegado de Protección de Datos** en los siguientes casos:

- 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 RGPD da la opción a los estados miembros de marcar la obligación de DPD en otros casos. En España el **Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal (PLOPD)** en lo relativo a nuestro ámbito, añade la obligación **para los centros sanitarios.** Aún es un proyecto de ley y no será definitivo por tanto hasta mayo, pero de momento si está prevista esa obligación de delegado de protección de datos en los centros sanitarios.

Así mismo también da la posibilidad de que se opte por contar con un delegado de protección de datos de forma voluntaria, para garantizar el cumplimiento del reglamento y evitar también las elevadas sanciones que marca el nuevo reglamento.

Para más información sobre el DPD, su cualificación y funciones se pueden consultar el siguiente enlace.

Transferencias internacionales

Es muy importante comprobar que los servidores de datos de todos los servicios que utilicemos estén situados en territorio europeo, para así garantizar que cumplen con las medidas de seguridad exigidas por la legislación de protección de datos, pero es posible que se realice en países fuera del territorio europeo. Eso sí, no todos los países tienen la misma exigencia en este tema, por lo que habrá que verificar cuidadosamente a qué países va ir la información.

La Guía del Reglamento de Protección de Datos para Responsables de tratamiento indica los siguientes casos en los que es posible transferir datos 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.
- 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.

En este enlace se puede encontrar más información sobre transferencias internacionales.

Para verificar todos los aspectos relacionados a la protección de datos proactiva se puede reflexionar sobre los siguientes aspectos:

¿Ha revisado las medidas de seguridad que aplica a sus tratamientos a la luz de los resultados del análisis de riesgo de los mismos?

¿Considera que puede seguir aplicando las medidas de seguridad previstas en el Reglamento de la LOPD?

¿Ha valorado suficientemente la posibilidad de introducir medidas adicionales en función del tipo de tratamiento o del contexto en que se realiza?

Atendiendo al tipo de tratamientos que realiza, ¿ha establecido mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos?

¿Tiene previstas medidas de reacción frente a los diferentes tipos de quiebras de seguridad, incluidos los procedimientos para evaluar el riesgo que puedan suponer para los derechos y libertades de los afectados?

¿Ha establecido procedimientos para notificar las violaciones de seguridad a las autoridades de protección de datos y, si fuera necesario, a los interesados?

¿Dispone de un registro o herramienta similar en que pueda documentar los incidentes de seguridad que se produzcan, aunque no sean notificados a las autoridades de protección de datos?

¿Ha valorado si los tratamientos que realiza requieren una Evaluación de Impacto sobre la Protección de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados?

¿Dispone de una metodología para la realización de la Evaluación de Impacto?

Según el tipo de tratamiento que realiza y los resultados del análisis de riesgos previo, ¿tiene que nombrar un Delegado de Protección de Datos?

¿Ha establecido los criterios para seleccionar al Delegado de Protección de Datos y, en particular, para valorar sus cualificaciones profesionales y sus conocimientos?

El puesto de DPD tal y como está configurado en su organización, ¿respeta los requisitos de independencia en el ejercicio de las funciones, posición en el organigrama, ausencia de conflicto de intereses y disponibilidad de los recursos necesarios establecidos por el RGPD?

¿Ha hecho pública la designación del DPD y sus datos de contacto y los ha comunicado a la autoridad de protección de datos?

¿Ha establecido procedimientos para que los interesados contacten con el DPD?