GUÍA DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS PARA RESPONSABLES DE TRATAMIENTO

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

apdcat
Autoritat Catalana de Protecció de Dades

Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

GUÍA DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS PARA RESPONSABLES DE TRATAMIENTO

Índice

1.- INTRODUCCIÓN

El nuevo **Reglamento General de Protección de Datos (RGPD)** fue publicado en mayo de 2016 y **será aplicable a partir de mayo de 2018**. En este periodo transitorio y aun cuando siguen vigentes las disposiciones de la Directiva 95/46 y las correspondientes normas nacionales de desarrollo, los responsables y encargados de tratamiento deben ir **preparando y adoptando las medidas necesarias** para estar en condiciones de cumplir con las previsiones del RGPD en el momento en que sea de aplicación.

El RGPD es una norma directamente aplicable, que no requiere de normas internas de trasposición ni tampoco, en la mayoría de los casos, de normas de desarrollo o aplicación. Por ello, **los responsables deben ante todo asumir que la norma de referencia es el RGPD y no las normas nacionales**, como venía sucediendo hasta ahora con la Directiva 95/46. No obstante, la ley que sustituirá a la actual Ley Orgánica de Protección de Datos (LOPD) sí podrá incluir algunas precisiones o desarrollos en materias en las que el RGPD lo permite.

El RGPD contiene muchos conceptos, principios y mecanismos similares a los establecidos por la Directiva 95/46 y por las normas nacionales que la aplican. Por ello, las organizaciones que en la actualidad cumplen adecuadamente con la LOPD española tienen una buena base de partida para evolucionar hacia una correcta aplicación del nuevo Reglamento.

Sin embargo, el RGPD **modifica algunos aspectos del régimen actual y contiene nuevas obligaciones** que deben ser analizadas y aplicadas por cada organización teniendo en cuenta sus propias circunstancias.

Dos elementos de carácter general constituyen **la mayor innovación del RGPD** para los responsables:

El principio de responsabilidad proactiva

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 enfoque de riesgo

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.

En esta Guía se presentan de forma sistemática **las principales cuestiones que las organizaciones deberán tener en cuenta de cara a la aplicación del RGPD**. No trata de ser un documento exhaustivo ni definitivo. Está pensada para ayudar a los responsables y a los encargados a adaptarse a las nuevas obligaciones durante el periodo transitorio hasta mayo de 2018. Por ello, al final de la Guía se incluye una Lista de Verificaciones que las organizaciones pueden utilizar para determinar si han dado los pasos necesarios para estar en condiciones de hacer una correcta aplicación del RGPD.

En algunos casos, las recomendaciones o interpretaciones que se ofrecen en la Guía pueden ponerse en práctica de forma casi inmediata, porque tienen que ver con actuaciones que debieran iniciarse ya durante el periodo de dos años entre la entrada en vigor y la aplicación del RGPD. Un ejemplo, como luego se verá, sería el de la adaptación del modo de obtención del consentimiento.

En otros casos, esas recomendaciones o propuestas solo deberán tenerse en cuenta en el momento en que el RGPD sea de aplicación. Su inclusión en la Guía obedece fundamentalmente al propósito de que las organizaciones vayan asumiendo la idea de que deberán adoptar determinadas medidas o seguir determinados criterios y ofrecer una primera aproximación al modo en que debería hacerlo, de forma que puedan ir anticipando la puesta en práctica a partir del momento en que sea ya legalmente obligatorio.

La Agencia Española de Protección de Datos junto con la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos está preparando, o han publicado ya, diversos documentos y herramientas que complementan esta Guía y que desarrollan más ampliamente algunas de sus secciones. Este catálogo de recursos dirigidos a la puesta en marcha de la nueva normativa se ampliará a lo largo de 2017 y 2018. En ese periodo también se producirán actualizaciones o ampliaciones de esta Guía.

2.- BASES DE LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS

El RGPD 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

En ese sentido, el RGPD no implica cambios para los responsables del tratamiento de datos.

A tener en cuenta

Documentar e identificar claramente la base legal sobre la que se desarrollan los tratamientos

- Aunque no está expuesto de forma explícita, se deduce de algunos artículos y del principio general de "responsabilidad activa".
    - Hay que **incluir la base legal sobre la que se desarrolla el tratamiento** al proporcionar la información en el momento de recoger los datos de los interesados.
    - Hay que **especificar y documentar los intereses legítimos en que se fundamenten las operaciones de tratamiento** en casos como los de las Evaluaciones de Impacto sobre la Protección de Datos o determinadas transferencias internacionales.
- **La identificación de la base legal es indispensable** para estar en condiciones de demostrar que se cumple con las previsiones del RGPD.
- La identificación documentación **debe adaptarse al tipo de tratamiento y a las características de las organizaciones.**

El consentimiento debe ser "inequívoco"

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

A diferencia del **Reglamento de Desarrollo de la LOPD**, no se admiten formas de consentimiento tácito o por omisión, ya que se basan en la inacción.

- Se contemplan situaciones en las que **el consentimiento, además de inequívoco, ha de ser explícito.**
    - Tratamiento de datos sensibles
    - Adopción de decisiones automatizadas
    - Transferencias internacionales
- El consentimiento **puede ser inequívoco y otorgarse de forma implícita** cuando se deduzca de una acción del interesado (por ejemplo, cuando el interesado continúa navegando por una web y acepta así el que se utilicen cookies para monitorizar su navegación).
- Los **tratamientos iniciados con anterioridad** al inicio de la aplicación del RGPD sobre la base del consentimiento seguirán siendo legítimos siempre que ese consentimiento se hubiera prestado del modo en que prevé el propio RGPD, es decir, mediante una manifestación o acción afirmativa.

Recomendaciones

- **No seguir obteniendo consentimiento por omisión** y revisar esos tratamientos para que, a partir mayo de 2018, se hayan adecuado a las previsiones del RGPD.
- La **adaptación** puede llevarse a cabo:
    - **Obteniendo un consentimiento de los interesados acorde con las disposiciones del RGPD**.
    - **Valorando si los tratamientos afectados pueden apoyarse en otra base legal** como puede ser, entre otras, el interés legítimo del responsable o del cesionario de los datos que prevalezca sobre los derechos del interesado (los interesados deben ser informados y podrán ejercitar los derechos que, como el de oposición, sean específicamente aplicables a la nueva base legal elegida).

3.- TRANSPARENCIA E INFORMACIÓN A LOS INTERESADOS

Cambios

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

  (La LOPD sólo exige que la información se preste de modo expreso, preciso e inequívoco)

Obligaciones

- Se deberán **evitar las fórmulas especialmente farragosas** y que incorporan remisiones a los textos legales
- Las **cláusulas informativas** deberán explicar el contenido al que inmediatamente se refieren de forma **clara y accesible para los interesados**, con independencia de sus conocimientos en la materia.
- Se establece una lista exhaustiva de los contenidos de la información que debe proporcionarse a los interesados (más amplia que la que actualmente contiene la LOPD) y que añade:
- Base jurídica del tratamiento
- Intención de realizar transferencias internacionales
- Datos del Delegado de Protección de Datos (si lo hubiere)
- Elaboración de perfiles
- La **información a los interesados deberá facilitarse por escrito**, incluidos, los medios electrónicos cuando sea apropiado.

Iconos estandarizados

La importancia que el RGPD concede a la claridad y accesibilidad de la información se refleja en el hecho de que prevé que pueda proporcionarse en combinación con iconos estandarizados que ofrezcan una visión de conjunto del tratamiento previsto. El diseño de estos iconos deberá hacerlo la Comisión Europea, que está ya trabajando para presentar una propuesta.

❖ **La AEPD, la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos han preparado una Guía sobre el derecho a la información que puede consultarse aquí. Durante el periodo transitorio se presentarán igualmente directrices para entidades privadas.**

4.- DERECHOS

El RGPD contiene los ya tradicionales derechos ARCO y también algunos nuevos derechos. Además, establece condiciones concretas sobre el procedimiento a seguir para atender al ejercicio de sus derechos.

4.1 Procedimiento para el ejercicio

- Con carácter general, **los responsables deben facilitar a los interesados el ejercicio de sus derechos**, y los procedimientos y las formas para ello deben ser visibles, accesibles y sencillos.
    - Se requiere que los responsables posibiliten la presentación de solicitudes por medios electrónicos, especialmente cuando el tratamiento se realiza por esos medios.
- **El ejercicio de los derechos será gratuito** para el interesado, excepto:
    - En los casos en que se formulen solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas, cuando el responsable podrá cobrar un canon que compense los costes administrativos de atender a la petición o negarse a actuar(el canon no podría implicar un ingreso adicional para el responsable, sino que debería corresponderse efectivamente con el verdadero coste de la tramitación de la solicitud).

Obligaciones

- Articular procedimientos que permitan fácilmente que los interesados puedan acreditar que han ejercido sus derechos por medios electrónicos (actualmente, en muchas ocasiones, no es viable.
- El responsable el que debe demostrar el carácter infundado o excesivo de las solicitudes que tengan un coste para el interesado.
- El responsable deberá informar al interesado sobre las actuaciones derivadas de su petición dentro del plazo de **un mes** (podrá extenderse dos meses más cuando se trate de **solicitudes especialmente complejas** y deberá notificar esta ampliación dentro del primer mes).
- Si el responsable decide **no atender una solicitud**, deberá informar de ello, motivando su negativa, dentro del plazo de **un mes** desde su presentación.
- Los responsables deberán tomar **medidas para verificar la identidad** de quienes soliciten acceso y de quienes ejerzan los restantes derechos ARCO.
- El responsable que trate una gran cantidad de información sobre un interesado podrá pedir a éste que especifique la información a que se refiere su solicitud de acceso.

- El responsable podrá contar con la **colaboración de los encargados** para atender al ejercicio de derechos de los interesados, pudiendo incluir esta colaboración en el contrato de encargo de tratamiento.

4.2 Derecho de acceso

ANTES

Debían facilitarse todos los datos de base del afectado, pero no copias o documentos (excepto en el caso de la historia clínica).

DESPUÉS

Se reconoce el derecho a obtener una copia de los datos personales objeto del tratamiento. Derecho de acceso.

A tener en cuenta

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

4.3 Derecho al olvido

- No está considerado un derecho autónomo o diferenciado de los clásicos derechos ARCO, sino la **consecuencia de la aplicación del derecho al borrado** de los datos personales.
- Es una **manifestación de los derechos de cancelación u oposición en el entorno online** (según la jurisprudencia que el Tribunal de Justicia de la UE estableció en el caso Google Spain).

A tener en cuenta

- Los responsables que actualmente aplican esta jurisprudencia no tienen que introducir ningún tipo de modificación en sus prácticas.
- Los responsables que hayan hecho públicos los datos personales deberán adoptar **medidas técnicas para informar a otros responsables** de la solicitud del interesado de borrar su información personal.

4.4 Limitación de tratamiento

Cambios

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

  Se puede solicitar la limitación cuando:

  - El interesado ha ejercido los derechos de rectificación u oposición y mientras el responsable determina si procede atender a la solicitud.
  - El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello.
  - Los datos ya no son necesarios para el tratamiento, lo que nuevamente determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.
- **En el tiempo que dure la limitación, el responsable sólo podrá tratar los datos afectados**, más allá de su conservación:
  - Con el consentimiento del interesado
  - Para la formulación, el ejercicio o la defensa de reclamaciones
  - Para proteger los derechos de otra persona física o jurídica
  - Por razones de interés público importante de la Unión o del Estado miembro correspondiente

A tener en cuenta

- La limitación de tratamiento se presenta en el RGPD como **un derecho de los interesados** que no debe confundirse con el bloqueo de datos actualmente existente en la legislación española.
- A este derecho se le aplican los mismos **plazos y procedimientos** que a los restantes derechos previstos en el RGPD.
- Como consecuencia de esta regulación, se impide la práctica habitual consistente en borrar los datos cuando se ejercitan otros derechos, como el de acceso, ya que impediría el ejercicio del derecho a la limitación del tratamiento.

4.5 Portabilidad

Cambios

- El derecho a la portabilidad de los datos es una forma avanzada del derecho de acceso por el cual **la copia que se proporciona al interesado debe ofrecerse en un formato estructurado, de uso común y lectura mecánica.**

  Este derecho sólo puede ejercerse:

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

A tener en cuenta

- El derecho a la portabilidad implica que los datos personales del interesado se transmitan directamente **de un responsable a otro**, sin necesidad de que sean transmitidos previamente al propio interesado, siempre que ello sea técnicamente posible.

  No es aplicable:

  - A los datos de terceras personas que un interesado haya facilitado a un responsable.
  - En caso de que el interesado haya solicitado la portabilidad de datos que le incumban pero que hayan sido proporcionados al responsable por terceros.

❖ **El Grupo de Autoridades Europeas de Protección de Datos (Grupo del Artículo 29) ha adoptado una opinión en la que se analiza detalladamente este derecho, que puede consultarse aquí**.

5.- RELACIONES RESPONSABLE – ENCARGADO

Hay 3 novedades que los responsables y encargados deben tomar en consideración

5.1 Obligaciones específicas para los encargados

ANTES

La Directiva 95/46 y en general las leyes nacionales de trasposición se centran en la actividad de los responsables.

DESPUÉS

El RGPD, por el contrario, contiene **obligaciones expresamente dirigidas a los encargados**.

La responsabilidad última sobre el tratamiento sigue estando atribuida al responsable, que es quien determina la existencia del tratamiento y su finalidad.

Cambios

- En determinadas materias **los encargados tienen obligaciones propias** que establece el RGPD, que no se circunscriben al ámbito del contrato que los une al responsable y que pueden ser supervisadas separadamente por las autoridades de protección de datos. Por ejemplo:
  - Deben mantener un registro de actividades de tratamiento.
  - Deben determinar las medidas de seguridad aplicables a los tratamientos que realizan.
  - Deben designar a un Delegado de Protección de Datos en los casos que prevé el RGPD.
- Los encargados **pueden adherirse a códigos de conducta o certificarse** en el marco de los esquemas de certificación previstos en el propio RGPD.

5.2 Elección del encargado de tratamiento

ANTES

El Reglamento de Desarrollo de la LOPD ya establece la necesidad de diligencia debida en la selección de encargados.

DESPUÉS

Según el RGPD el responsable deberá adoptar las medidas apropiadas, incluida la elección de encargados, de forma que garantice y esté en condiciones de demostrar que el tratamiento se realiza conforme al RGPD (principio de responsabilidad activa).

Cambios

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

Recomendaciones

- Para demostrar que los encargados o subencargados ofrecen las garantías exigidas por el RGPD, estos podrán adherirse a códigos de conducta o certificarse dentro de los esquemas previstos por el RGPD.

5.3 Contenido del contrato de encargo

Cambios

- Las relaciones entre el responsable y el encargado deben formalizarse en **un contrato o en un acto jurídico** que vincule al encargado respecto al responsable.
- Se regula de forma minuciosa el **contenido mínimo que han de tener los contratos** de encargo, debiendo preverse aspectos como:
    - Objeto, duración, naturaleza y la finalidad del tratamiento
    - Tipo de datos personales y categorías de interesados
    - 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
    - Asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados…

Obligaciones

Los **contratos de encargo concluidos con anterioridad a la aplicación del RGPD en mayo de 2018 deben adaptarse para respetar este contenido**, sin que sean válidas las remisiones genéricas al artículo del RGPD que los regula.

- **La AEPD, la APDCAT y la AVPD han preparado unas directrices para la redacción de estos contratos que pueden consultarse aquí. Estas directrices están pensadas para ayudar a responsables y encargados durante el periodo transitorio hasta la entrada en aplicación del RGPD. Posteriormente, y de acuerdo con lo previsto en el Reglamento, la AEPD podrá elaborar clausulados modelo que deberán ser aprobados por el futuro Comité Europeo de Protección de Datos. La Comisión Europea también podrá preparar cláusulas contractuales modelo.**

6.- MEDIDAS DE RESPONSABILIDAD ACTIVA

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.

6.1 Análisis de riesgo

- El RGPD **condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados**. Se maneja el riesgo de dos maneras:
    - En algunos casos, prevé que determinadas medidas sólo deberán aplicarse cuando el tratamiento suponga un alto riesgo para los derechos y libertades (por ejemplo, Evaluaciones de Impacto sobre la Protección de Datos).
    - En otros casos, las medidas a aplicar deberán modularse en función del nivel y tipo de riesgo que el tratamiento conlleve. Esto ocurre, por ejemplo, con las medidas de Protección de Datos desde el Diseño o con las medidas de seguridad.

Obligaciones

- Todos los **responsables deberán realizar una valoración del riesgo** de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo. El tipo de análisis variará en función de:
    - los tipos de tratamiento,
    - la naturaleza de los datos que se traten,
    - el número de interesados afectados,
    - la cantidad y variedad de tratamientos que una misma organización lleve a cabo.

Grandes organizaciones: como regla general, el análisis deberá llevarse a cabo utilizando alguna de las metodologías de análisis de riesgo existentes.

Organizaciones de menor tamaño y con tratamientos de poca complejidad: el análisis será el resultado de una reflexión, mínimamente documentada, sobre las implicaciones de los tratamientos en los derechos y libertades de los interesados. La reflexión deberá dar respuesta a cuestiones como las que se exponen a continuación. Cuanto mayor sea el número de respuestas afirmativas mayor sería el riesgo que podría derivarse del tratamiento. Si la respuesta a estas preguntas y otras del mismo tipo fuera negativa, es razonable concluir que la organización no realiza tratamientos que generen un elevado nivel de riesgo y que, por tanto, no debe poner en marcha las medidas previstas para estos casos.

- ¿Se tratan datos sensibles?
- ¿Se tratan datos de una gran cantidad de personas?
- ¿Incluye el tratamiento la elaboración de perfiles?

- ¿Se cruzan los datos obtenidos de los interesados con otros disponibles en otras fuentes?
- ¿Se pretende utilizar los datos obtenidos para una finalidad para otro tipo de finalidades?
- ¿Se están tratando grandes cantidades de datos, incluido con técnicas de análisis masivo tipo big data?
- ¿Se utilizan tecnologías especialmente invasivas para la privacidad, como las relativas a geolocalización, videovigilancia a gran escala o ciertas aplicaciones del Internet de las Cosas?...

❖ **La AEPD está desarrollando materiales para ayudar a las PYMES a adaptarse a las nuevas especificaciones del Reglamento, en particular en relación con el proceso de valoración de los riesgos en tratamientos que, a priori, no parezcan generar alto riesgo.**

6.2 Registro de actividades de tratamiento

Obligaciones

- **Responsables y encargados** deberán mantener un **registro de operaciones de tratamiento** en el que se contenga toda la información que el RGPD establece. Esta información incluye cuestiones como:
  - Nombre y datos de contacto del responsable y, en su caso, corresponsable, así como del Delegado de Protección de Datos si existiese
  - Finalidades del tratamiento
  - Descripción de categorías de interesados y categorías de datos personales tratados
  - Transferencias internacionales de datos…
- Están **exentas las organizaciones que empleen a menos de 250 trabajadores**, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

Recomendaciones

- Las **posibilidades para organizar el registro de actividades de tratamiento** son:
  - Partir de los ficheros que actualmente tienen notificados los responsables en el Registro General de Protección de Datos, detallando todas las operaciones que se realizan sobre cada conjunto estructurado de datos.
  - En torno a 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.

- **Con la finalidad de facilitar a los responsables la constitución de estos registros, la AEPD, la APDCAT y la AVPD permitirán, con antelación suficiente a la fecha de aplicación del RGPD, que los responsables puedan obtener de forma automatizada toda la información que sobre sus propios ficheros o tratamientos hayan notificado al Registro General.**

6.3 Protección de Datos desde el Diseño y por Defecto

Estas medidas se incluyen dentro de las que debe aplicar el responsable **con anterioridad al inicio del tratamiento y también cuando se esté desarrollando.**

Este tipo de medidas reflejan muy directamente el enfoque de responsabilidad proactiva. Se trata de **pensar en términos de protección de datos desde el mismo momento en que se diseña un tratamiento**, o un producto o servicio que implica el tratamiento de datos personales.

Obligaciones

- Desde el principio **los responsables deben tomar medidas organizativas y técnicas** para integrar en los tratamientos, garantías que permitan aplicar de forma efectiva los principios del RGPD.
- Los responsables deben adoptar **medidas que garanticen que se traten sólo los datos necesarios** en lo relativo a la cantidad de datos tratados, la extensión del tratamiento, los periodos de conservación y la accesibilidad a los datos.

6.4 Medidas de seguridad

ANTES

El Reglamento de Desarrollo de la LOPD determinaba con detalle y de forma exhaustiva las medidas de seguridad que deben aplicarse según el tipo de datos que sean objeto de tratamiento.

Las medidas del Reglamento de la LOPD estaban basadas casi exclusivamente en el tipo de datos que se trataban, con alguna matización relativa al contexto en que se llevan a cabo los tratamientos.

AHORA

En el RGPD los responsables y encargados establecerán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo

El RGPD pide que se tomen en consideración más variables.

A tener en cuenta

- Las medidas **técnicas y organizativas deberán establecerse** teniendo en cuenta:
  - el coste de la técnica
  - los costes de aplicación
  - la naturaleza, el alcance, el contexto y los fines del tratamiento
  - los riesgos para los derechos y libertades
- El esquema de medidas de seguridad previsto en el Reglamento de Desarrollo de la LOPD **no seguirá siendo válido de forma automática** tras la fecha de aplicación del RGPD.
- **En algunos casos los responsables podrán seguir aplicando las mismas medidas** que establece el Reglamento de la LOPD si los resultados del análisis de riesgos concluye que las medidas son realmente las más adecuadas para ofrecer un nivel de seguridad adecuado. En ocasiones será necesario completarlas con medidas adicionales o prescindir de alguna de las medidas.

6.5 Notificación de "violaciones de seguridad de los datos"

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 sus 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.

Obligaciones

- **Cuando se produzca una violación de la 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.**
- La **notificación de la quiebra** a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.
- La notificación ha de incluir un contenido mínimo:
  - la naturaleza de la violación,
  - categorías de datos y de interesados afectados,

- medidas adoptadas por el responsable para solventar la quiebra,
- si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados

- **Los responsables deben documentar todas las violaciones de seguridad.**
- En los casos en que sea probable que la **violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados**, la notificación a la autoridad de supervisión deberá complementarse con una **notificación dirigida a estos últimos.**
- El **objetivo de la notificación a los afectados** es permitir que puedan tomas medidas para protegerse de sus consecuencias. Por ello, el RGPD requiere que se realice sin dilación indebida, sin hacer referencia ni al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas. El propósito es siempre que el interesado afectado pueda reaccionar tan pronto como sea posible.
- El RGPD añade a los contenidos de la notificación **las recomendaciones sobre las medidas que pueden tomar los interesados** para hacer frente a las consecuencias de la quiebra.

A tener en cuenta

- La **valoración del riesgo de la quiebra es distinta del análisis de riesgos previo** a todo tratamiento. Se trata de establecer hasta qué punto el incidente, por sus características, el tipo de datos a los que se refiere o el tipo de consecuencias que puede tener para los afectados puede causar un daño en sus derechos o libertades.
- **Los daños pueden ser** materiales o inmateriales, e ir desde la posible discriminación de los afectados como consecuencia de su uso por quien ha accedido a ellos de forma no autorizada hasta usurpación de identidad, pasando por perjuicios económicos o la exposición pública de datos confidenciales.
- Se considera que **se tiene constancia de una violación de seguridad cuando** hay una certeza de que se ha producido y se tiene un conocimiento suficiente de su naturaleza y alcance.
- La mera **sospecha de que ha existido una quiebra** o la constatación de que ha sucedido algún tipo de incidente sin que se conozcan mínimamente sus circunstancias no deberían dar lugar, todavía, a la notificación, dado que en esas condiciones no sería posible, en la mayoría de los casos, determinar hasta qué punto puede existir un riesgo para los derechos y libertades de los interesados.
- En casos de **quiebras que por sus características pudieran tener gran impacto**, sí podría ser recomendable contactar con la autoridad de supervisión tan pronto como existan evidencias de que se ha producido alguna situación irregular respecto a la seguridad de los datos, sin perjuicio de que esos primeros contactos puedan completarse con una notificación formal más completa dentro del plazo legalmente previsto.
- Puede haber **casos en que la notificación no pueda realizarse dentro de esas 72 horas**, por ejemplo, por la complejidad en determinar completamente su alcance. En esos casos,

es posible hacer la notificación con posterioridad, acompañándola de una explicación de los motivos que han ocasionado el retraso.

- La información puede proporcionarse **de forma escalonada** cuando no sea posible hacerlo en el mismo momento de la notificación.
- El **criterio de alto riesgo** debe entenderse en el sentido de que sea probable que la violación de seguridad ocasione daños de entidad a los interesados. Por ejemplo, en casos en que se desvele información confidencial, como contraseñas o participación en determinadas actividades, se difundan de forma masiva datos sensibles o se puedan producir perjuicios económicos para los afectados.
- La **notificación a los interesados no será necesaria** cuando:
  - El responsable hubiera tomado medidas técnicas u organizativas apropiadas con anterioridad a la violación de seguridad, en particular las medidas que hagan ininteligibles los datos para terceros, como sería el cifrado.
  - Cuando el responsable haya tomado con posterioridad a la quiebra medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice.
  - Cuando la notificación suponga un esfuerzo desproporcionado, debiendo en estos casos sustituirse por medidas alternativas como puede ser una comunicación pública.

❖ **La AEPD estableció en su momento un canal específico para la notificación de las quiebras de seguridad en el ámbito de las comunicaciones electrónicas, único en que hasta ahora resultaba obligatoria la notificación en aplicación de las previsiones de la Directiva 2002/58 y la normativa nacional de trasposición. Durante el periodo transitorio hasta la aplicación del RGPD la AEPD adaptará este canal para que pueda ser utilizado para la comunicación de las violaciones de seguridad en el marco del RGPD.**

Asimismo, el Grupo del Artículo 29 preparará un formulario estandarizado a nivel europeo tanto para ayudar a los responsables a presentar unas notificaciones completas de acuerdo con los criterios del RGPD como para que esas notificaciones se realicen de forma armonizada a en toda la Unión Europea.

6.6 Evaluación de Impacto sobre la Protección de Datos

Obligaciones

- **Los responsables de tratamiento deberán realizar una Evaluación de Impacto sobre la Protección de Datos** (EIPD) con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados.
- El RGPD establece un **contenido mínimo de las Evaluaciones de Impacto sobre la Protección de Datos**, aunque no contempla ninguna metodología específica para su realización. La AEPD publicó en 2014 una Guía sobre estas Evaluaciones que será

actualizada y publicada durante el periodo transitorio para incorporar las novedades del RGPD.

- Cuando el análisis de riesgo que las organizaciones lleven a cabo sobre los **tratamientos iniciados con anterioridad a la fecha de aplicación del RGPD** indiquen que esos tratamientos presentan alto riesgo para los derechos o libertades de los interesados, los responsables deberán realizar una EIPD sobre esos tratamientos, a fin de estar en condiciones de poder adoptar las medidas adecuadas para adecuar esos tratamientos a las exigencias del RGPD.
- En los casos en que las EIPD hayan identificado un **alto riesgo que a juicio del responsable de tratamiento no pueda mitigarse por medios razonables en términos de tecnología disponible y costes de aplicación, el responsable deberá consultar a la autoridad de protección de datos competente.** La consulta debe ir acompañada de la documentación que prevé el RGPD, incluyendo la propia Evaluación de Impacto, y la autoridad de supervisión puede emitir recomendaciones o ejercer cualquiera otro de los poderes que el RGPD le confiere, entre ellos el de prohibir la operación de tratamiento.

A tener en cuenta

- **Lista indicativa de supuestos en que se considera que los tratamientos conllevan un 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
  - Tratamiento a gran escala de datos sensibles
  - Observación sistemática a gran escala de una zona de acceso público
- Para **valorar si un tratamiento se realiza a gran esc**ala 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
- **Las autoridades de protección de datos están obligadas a confeccionar listas adicionales de tratamientos que requerirán una EIPD**. La AEPD, la ACTPD y la AVPD elaborarán esa lista con anterioridad a la aplicación del RGPD, dado que tiene que ser sometida a la aprobación del futuro Comité Europeo de Protección de Datos y éste sólo se constituirá a partir de la fecha de aplicación del RGPD.
- También **está prevista que las autoridades puedan elaborar listas de tratamientos en que no se precisa EIPD**. La AEPD, la ACTPD y la AVPD elaborarán esa lista en las mismas condiciones que la correspondiente a tratamientos en que deberá realizar Evaluación.

- **La existencia de estos listados no excluye el que los responsables deban realizar el correspondiente análisis de riesgo** y, en caso de que concluyan que existe un alto riesgo para los derechos y libertades de los interesados, lleven a cabo una EIPD, aun cuando el tratamiento en cuestión no esté incluido en ninguna de las dos listas mencionadas. Como se ha dicho, el RGPD se basa en un principio de responsabilidad activa del responsable y es siempre en último extremo el responsable el que debe decidir qué medidas aplicar y cómo hacerlo. La intervención de las autoridades de supervisión o las previsiones del propio RGPD aclaran sus disposiciones o las especifican, pero no sustituyen la responsabilidad de quienes tratan los datos.
- Es posible realizar **una única EIPD para varios tratamientos similares** que entrañen altos riesgos también similares.
- Puede ser necesario llevar a cabo una nueva Evaluación **cuando cambien las condiciones del tratamiento o cuando varíen los riesgos** asociados al mismo.

❖ **Al margen de las listas expresamente previstas por el RGPD, la AEPD, la APDCAT y la AVPD publicarán durante el periodo transitorio herramientas que ayuden a las empresas a determinar la necesidad de realizar EIPD.**

Igualmente, el Grupo del Artículo 29 prepara un dictamen, que se publicará en el primer semestre de 2017, sobre la noción de alto riesgo asociada a la obligatoriedad de llevar a cabo Evaluaciones de Impacto.

6.7 Delegado de Protección de Datos

Obligaciones

- 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**. Esto no significa que el DPD deba tener una titulación específica. En la medida en que entre las funciones del DPD se incluye 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 encuentra:
  - total autonomía en el ejercicio de sus funciones
  - necesidad de que se relacione con el nivel superior de la dirección
  - la obligación de que el responsable o el encargado faciliten al DPD todos los recursos necesarios para desarrollar su actividad.

A tener en cuenta

- Se permite **nombrar un solo DPD para un grupo empresarial** siempre que sea accesible desde cada establecimiento del grupo. La noción de 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 tan 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 de 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.

- El RGPD prevé también el **catálogo de funciones del DPD**, entre las que se incluyen las relativas a actuar como punto de contacto para los interesados en todo lo que tenga relación con el tratamiento de sus datos personales.

❖ **El Grupo del Artículo 29 ha publicado un dictamen sobre la designación de los DPD que puede consultarse aquí, en el que pueden encontrarse también una serie de Preguntas Frecuentes sobre los diversos aspectos de esta figura.**

7.- TRANSFERENCIAS INTERNACIONALES

El modelo de transferencias internacionales diseñado por el RGPD sigue los mismos criterios que el establecido por la Directiva 95/46 y por las legislaciones nacionales de trasposición.

Obligaciones

- **Los datos sólo 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
    - 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 tener en cuenta

Desde el punto de vista de los responsables y encargados que actualmente realizan transferencias internacionales o que las efectuarán en el marco del RGPD:

- Las **decisiones de adecuación** que la Comisión ha adoptado con anterioridad a la aplicación del RGPD seguirán siendo válidas, y por tanto podrán seguir realizándose transferencias basadas en ellas, en tanto la Comisión no las sustituya o derogue.
- Las decisiones de la Comisión estableciendo **cláusulas tipo para los contratos** en los que se establecen garantías para las transferencias internacionales seguirán siendo válidas hasta que la Comisión las sustituya o derogue.
- Las **autorizaciones de transferencias** que las autoridades nacionales de protección de datos hayan otorgado sobre la base de garantías contractuales seguirán siendo válidas en tanto las autoridades no las revoquen.
- Las **garantías sobre la protección que recibirán los datos en destino** las debe ofrecer el exportador, que podrá ser tanto un responsable como un encargado de tratamiento.
- Se amplía la **lista de posibles instrumentos para ofrecer garantías**, incluyéndose expresamente, entre otros, las Normas Corporativas Vinculantes para responsables y encargados, los códigos de conducta y esquemas de certificación, así como los cláusulas contractuales modelo que puedan aprobar las autoridades de protección de datos.
- En los casos de **Normas Corporativas Vinculantes, cláusulas contractuales estándar, códigos de conducta y esquemas de certificación**, la transferencia no requerirá la autorización de las autoridades de supervisión.
- 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.

8.- TRATAMIENTOS DE DATOS DE MENORES

El RGPD se refiere en varios lugares a los tratamientos de los datos de los menores:

- En la regulación de los intereses legítimos del responsable como base legal para el tratamiento, señalándose que no será aplicable cuando prevalezcan los derechos, libertades o intereses de los interesados que requieran protección de datos personales, especialmente cuando esos interesados sean niños.
- Al señalar que la información que se ofrece a los interesados en relación con el tratamiento o con el ejercicio de derechos deberá ser especialmente concisa, transparente, inteligible y proporcionada con lenguaje claro y sencillo cuando los interesados sean niños
- En el contexto del derecho al borrado de los datos personales
- Al establecer que las actividades de formación y sensibilización dirigidas a los niños deberán estar entre las prioridades de las autoridades de protección de datos
- En el contexto de las explicaciones que ofrecen los Considerandos del RGPD cuando se refieren a la realización de perfiles

A tener en cuenta

- La mención más explícita a los menores (niños en la terminología del RGPD) está relacionada con la **obtención del consentimiento de los menores (niños, en la terminología del RGPD) en el ámbito de la oferta directa de servicios de la sociedad de la información**. El RGPD prevé que en este entorno **el consentimiento sólo será válido a partir de los 16 años**, debiendo contar con la autorización de los padres o tutores legales por debajo de esa edad.
- El RGPD **permite a los Estados Miembros establecer una edad inferior**, siempre que **no sea menor de 13 años.** Es de esperar que muchos Estados Miembros hagan uso de esta posibilidad y adopten regulaciones propias. En el caso de España el Reglamento de Desarrollo de la LOPD fija la edad a partir de la que el consentimiento de los menores es válido en los 14 años con carácter general. Por ello es razonable suponer que la norma que reemplace a la LOPD contenga también una regulación específica en esta materia.

Obligaciones

El RGPD requiere que los responsables hagan **esfuerzos razonables**, teniendo en cuenta la tecnología disponible, para verificar que, para los niños menores de la edad que se fije como límite, el consentimiento se ha dado o se ha autorizado por los padres o tutores del menor (no es una obligación en sí, sino tan sólo de medios o procedimientos razonables para establecer la intervención real de padres o tutores).

9.- LISTA DE VERIFICACIÓN

Esta **Lista de Verificación** pretende ayudar a las organizaciones a llevar a cabo de forma ordenada una valoración de su situación frente a las principales obligaciones del RGPD. Su contenido sigue el de la Guía, y se presenta como un listado de preguntas que responsables y encargados deberán formularse, y responder adecuadamente, a la hora de determinar cuál es su situación ante la aplicación del RGPD.

Legitimación

- ¿Tiene establecida claramente cuál es la base legal de los tratamientos que realiza y ha documentado de alguna forma el modo en que la ha establecido?
- Si alguno de los tratamientos que realiza está basado en el consentimiento de los interesados, ¿ha verificado que ese consentimiento reúne los requisitos que exige el RGDP? En caso contrario, ¿ha previsto cómo recabar el consentimiento de forma adaptada al RGPD o ha encontrado otra base legal adecuada para esos tratamientos?

Información y derechos

- La información que se proporciona a los interesados, ¿está presentada de forma clara, concisa, transparente y de fácil acceso?
- ¿Contiene esa información todos los elementos que prevé el RGPD?
- ¿Dispone de mecanismos para el ejercicio de derechos visibles, accesibles y sencillos? ¿Pueden ejercerse los derechos por vía electrónica?
- ¿Tiene establecidos procedimientos o mecanismos que le permitan verificar la identidad de quienes solicitan acceso o ejercen los demás derechos ARCO?
- ¿Tiene establecidos procedimientos que le permitan responder a los ejercicios de derechos en los plazos previstos por el RGPD? ¿Ha valorado si sería necesaria la colaboración de los encargados para responder a las solicitudes de los interesados y, si es así, tiene previsto incluir esta colaboración en los contratos de encargo?
- En particular, ¿tiene 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?
- ¿Ha valorado si los tratamientos de datos que realiza pueden ser objeto del derecho a la portabilidad? En caso, afirmativo, ¿ha 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

- ¿Ha previsto cómo valorar si los encargados con los que haya contratado o vaya a contratar operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD cuando sea de aplicación?
- ¿Contienen los contratos de encargo que actualmente tenga suscritos todos los elementos que prevé el RGPD? En caso contrario, ¿está dando pasos para adaptarlos antes de la aplicación del RGPD?

Medidas de responsabilidad proactiva

- ¿Ha hecho una valoración de los riesgos que los tratamientos que desarrolla implican para los derechos y libertades de los ciudadanos? ¿Ha determinado qué medidas de responsabilidad activa corresponden a su situación de riesgo y cómo debe aplicarlas?
- ¿Ha previsto cómo establecer el registro de actividades de tratamiento en su organización?
- ¿Ha valorado si le es de aplicación alguna de las excepciones a esta obligación? ¿Ha previsto quién se encargará de mantener actualizado el registro?
- ¿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?

10.- LISTA DE VERIFICACIÓN SIMPLIFICADA

Los responsables que realicen un número limitado de tratamientos que sea probable que presenten un bajo nivel de riesgo para los derechos y libertades de los interesados podrán simplificar la valoración de los aspectos relevantes a la hora de determinar que están en condiciones de aplicar adecuadamente el RGPD.

Estos responsables serán en muchos casos pymes o micropymes, aunque también pueden incluirse entre ellos organizaciones de mayor tamaño. El elemento realmente decisivo es el tipo de tratamientos que lleven a cabo. Empresas que realicen tratamientos básicos sobre los datos de sus empleados, clientes y proveedores, o comunidades de copropietarios que hagan tratamientos limitados a la gestión de las tareas propias de la comunidad, se encontrarían entre ellos.

Esta aproximación simplificada no sería válida para responsables que, con independencia de su tamaño, desarrollen tratamientos que impliquen un nivel de riesgo mayor. Por el tipo de tratamiento (por ejemplo, elaboración de perfiles), por el tipo de datos tratados (por ejemplo, uso de datos sensibles) o por el uso de determinados medios de tratamiento (por ejemplo, tecnologías de análisis masivo de información).

Para aplicar esta versión simplificada del Listado de Verificación, los responsables deberían ante todo confirmar que los tratamientos que realizan son de bajo riesgo y no tienen algún rasgo particular que elevaría ese nivel de riesgo.

A partir de ahí, podrían concentrar su análisis en las siguientes cuestiones:

Identificación de la base jurídica de los tratamientos que se realizan

Estos tratamientos básicos normalmente se basan en la existencia de una relación contractual entre el interesado o el responsable o en el consentimiento del interesado. También es habitual que existan obligaciones legales para el responsable, por ejemplo en el ámbito de la legislación laboral, que determinen el tratamiento de los datos. Puede haber algunos casos en que sea el interés legítimo del responsable. El responsable debe asegurarse de que todos los tratamientos que realiza pueden apoyarse en alguna de esas bases.

Verificación de la información que se proporciona a los interesados

El RGPD obliga a ofrecer a los interesados una mayor información sobre los tratamientos que se realizan. Todos los responsables han de cumplir con esta obligación de transparencia, con independencia de su tamaño como organización. Por ello, los responsables han de asegurarse de que disponen de esa información y han previsto los medios adecuados para ofrecerla a los interesados. Sin embargo, los responsables que utilicen esta Lista Simplificada, teniendo en cuenta el tipo de tratamientos que realizan, no tendrían en principio que informar sobre cuestiones tales como los datos de contacto del Delegado de Protección de Datos, o la adopción de decisiones automatizadas.

La información podrá proporcionarse por diversos medios, como son avisos en páginas webs, espacios reservados en formularios o carteles informativos. También podrá ofrecerse en diversos momentos, como por ejemplo cuando se recogen los datos de los empleados o cuando se recogen los datos para contratación con los clientes.

Establecimiento de un registro de actividades de tratamiento

El responsable debe prever la existencia de este registro e incluir en él los contenidos previstos por el RGPD. Si tiene ficheros notificados al Registro General de Datos, puede organizarlo relacionando los tratamientos con las finalidades con que notificó los ficheros.

Ejercicio de derechos de los interesados

El responsable debe prever mecanismos para facilitar el ejercicio de derechos y la respuesta a las solicitudes. Estos mecanismos dependerán de las entidades, pero pueden ser tan simples como establecer una dirección de correo electrónico específica que sea operativa y que permita identificar a los interesados y atribuir a una persona de la organización que se responsabilice de tramitar todas las solicitudes que eventualmente se reciban. No obstante, es importante que estos mecanismos, por sencillos que sean, estén claramente establecidos. El modo de ejercer los derechos forma parte de la información que debe proporcionarse a los interesados.

Identificación de medidas de seguridad

Las medidas de seguridad tienen como finalidades principales garantizar la integridad de la información, permitir su recuperación en caso de incidentes y evitar los accesos no autorizados a las mismas. Por ello, el RGPD contempla medidas de seguridad que deben adaptarse a las características de los tratamientos, al tipo de datos tratados o a la tecnología disponible en cada momento.

Los tratamientos que implican un bajo riesgo para los derechos o libertades de los interesados no requerirían, en principio, medidas de seguridad más complejas que las que actualmente establece el Reglamento de Desarrollo de la LOPD para el nivel básico. El responsable debe asegurarse de que esas medidas se aplican y también valorar si en el caso de los tratamientos que realiza, por ejemplo, por el contexto concreto en que se desarrollan o el tipo de interesados a que se refiere, sería necesaria alguna medida de seguridad distinta o adicional. En este caso, podrían servir como orientación las medidas de nivel medio que se recogen en el Reglamento de la LOPD.

Verificación de las relaciones con los encargados de tratamiento

Cuando el responsable del tratamiento encomienda parte de las operaciones, como puede ser el almacenamiento de la información o la realización de determinadas tareas sobre la base de los datos personales, la entidad que presta esos servicios es un encargado de tratamiento.

El responsable debería asegurarse, ante todo, de que estos encargos estén siempre amparados en un contrato de encargo, que tiene un contenido distinto del que regula el servicio que se contrata, aunque puede formar parte de él

Igualmente, debe verificar que los contratos de encargo de tratamiento con prestadores de servicios incluye todos los aspectos que establece el RGPD, especialmente en lo relativo a que el encargado sólo tratará los datos para los fines que le encomiende el responsable, que aplicará las medidas de seguridad adecuadas y que mantendrá estricta confidencialidad sobre la información tratada.

En algunos casos, el modelo de contrato será ofrecido por el prestador. Si es así, el responsable debe ser consciente de que al suscribirlo convierte su contenido en las instrucciones para el tratamiento y se responsabiliza de ellas. En otros casos, será el responsable el que pueda preparar el modelo de contrato. En estos supuestos, sería aconsejable que recurriera a los modelos ya aprobados por la Comisión Europea o presentados por las autoridades de protección de datos.

- **La AEPD está desarrollando herramientas específicamente dirigidas a facilitar a estas organizaciones, en particular pymes y micropymes, la valoración de la existencia de un bajo nivel de riesgo y el cumplimiento de los anteriores requisitos. Estas herramientas estarán disponibles en la página web de la AEPD.**