MEDIAS DE SEGURIDAD EN EL NUEVO RGPD.

27 de febrero de 2018

MEDIDAS DE SEGURIDAD. ENFOQUE DEL RIESGO

En la actual LOPD y su Reglamento de desarrollo, se establece tres niveles de seguridad (bajo, medio, alto) y de medidas de seguridad a adoptar (lista tasada) en función del **tipo** de datos de carácter personal que se traten, de manera que cuanto más sensibles sean los datos (salud, origen racial, religión, ideología, etc) mayor será el nivel de seguridad que se deba implementar en el tratamiento.

A partir del 25 de mayo de 2018, con la aplicación del nuevo RGPD, desaparece este criterio de "listas tasadas", y se produce un cambio sustancial al dejar en manos de las empresas y organizaciones que traten datos personales, la **responsabilidad de decidir y adoptar aquellas medidas de seguridad, que en atención al riesgo para la privacidad, derechos y libertades de las personas, sean las más adecuadas** (principio de responsabilidad proactiva).

¿Qué exige el nuevo Reglamento Europeo (RGPD)?

El Art. 5.f del RGPD exige que los datos personales sean:

> *"tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la **protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental**, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad, confidencialidad, disponibilidad, resilencia»)"*

Estas medidas deberán aplicarse **tanto a priori, como durante el proceso de tratamiento** donde **el responsable y el encargado del tratamiento** serán responsables del análisis de los posibles riesgos para la privacidad, de la adopción de las medidas acordes a dicho riesgo y de su cumplimiento; en todo caso, deberán ser capaces de demostrarlo (responsabilidad proactiva).

En consecuencia, las empresas y organizaciones deberán:

- ✓ **Analizar y revisar las medidas que actualmente tienen implementadas en su organización conforme a los nuevos principios del RGPD.**
- ✓ **Y antes de iniciar cualquier nuevo proceso, tratamiento, desarrollo de una nueva aplicación, o se destinen los datos a fines distintos a los inicialmente previstos, deberá realizarse un análisis del riesgo que tales actividades puedan suponer para la privacidad, derechos y libertades de los interesados.**

¿Qué criterios seguir a la hora de determinar las medidas que sean más adecuadas?

El RGPD introduce en su Artículo 25 el concepto de **"*protección de datos desde el diseño y por defecto*"** (recabar los datos mínimos y necesarios para los fines legítimos perseguidos con su tratamiento) de

manera que a la hora de adoptar de forma efectiva las medidas técnicas y organizativas para la protección de datos, se tenga en cuenta:

- Estado de la técnica
- Coste de la aplicación de la medida
- La naturaleza, ámbito, contexto y fines del tratamiento
- Los riesgos de probabilidad y gravedad que el tratamiento conlleve para los derechos y libertades de las personas físicas.

Por tanto, se establece la necesidad de realizar una efectiva **Gestión de Riesgos** con el fin de que las medidas de seguridad que se lleven a cabo garanticen la protección de los datos personales, valorando las amenazas que el tratamiento de los datos puedan suponer para los derechos y libertades de los interesados.

¿Cómo realizar el análisis de riesgos?

La AEPD recientemente ha publicado una Guía Práctica de Análisis de Riesgos en los tratamientos personales sujetos al RGPD, recomendando seguir los siguientes pasos:

1. **Identificar amenazas**: cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos de carácter personal se realiza un tratamiento.
2. **Evaluación de riesgos**: valorar el impacto de la exposición a la amenaza, junto a la probabilidad de que esta se materialice.
3. **Tratar los riesgos:** disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto de que estos se materialicen.

Ilustración 1 Fuente: AEPD

Aunque será abordado en otra publicación, es importante mencionar aquí, que tras este primer análisis, en el caso de hallar un **alto riesgo** para los derechos y libertades de los interesados, se deberá realizar un análisis adicional denominado "**evaluación de impacto relativa a la protección de datos**" (EIPD, en ingles Privacy Impact Assesment o PIA)

¿Qué tipo de medidas adoptar?

Las medidas a adoptar deberán ser de dos tipo:

A) Medidas Organizativas: al igual que se venía haciendo con la actual LOPD, la organización deberá disponer a nivel de gobierno de una política en materia de protección de datos personales (cultura de privacidad), y disponer de los contratos, clausulas, avisos legales, procedimientos necesarios para cumplir con el derecho de información, recogida del consentimiento, uso de las herramientas tecnológicas por los empleados, entre otras.

Como novedad el RGPD exige además:

1.- Contar con un procedimiento para la comunicación a la *Autoridad de Control* (Agencia Española de Protección de datos –AEPD-) las violaciones de seguridad de los datos personales que se puedan producir en el entorno de la empresa (en el plazo de 72 hs), y en determinados supuestos (alto riesgo) también a los propios *interesados*.

2.- Disponer de un mecanismo para la resolución de las *solicitudes formuladas por los interesados en el ejercicio de los derechos que les reconoce el RGPD* (antiguos derechos ARCO, y además derecho de limitación, derecho al olvido y portabilidad de los datos).

B) Medidas técnicas: para garantizar el nivel de seguridad adecuado al riesgo, el responsable y encargado del tratamiento deberán aplicar, entre otras, medidas de seudominimización y cifrado de datos personales, en aras a garantizar la confidencialidad, integridad, disponibilidad, resilencia de los datos y capacidad de restauración en caso de incidente físico o técnico.

La organización deberá disponer de un procedimiento de verificación, evaluación y valoración regulares de la eficacia de dichas medidas.

¿Cómo podemos demostrar el cumplimiento del RGPD?

El Reglamento establece en números apartados de su articulado, que *la adhesión a un **código de conducta** aprobado a tenor de su artículo 40 o a un **mecanismo de certificación, y de sellos y marcas** aprobado a tenor de su artículo 42 podrán servir de elementos para **demostrar** el cumplimiento del Reglamento*.

Por lo tanto, dos son las fórmulas que contempla el RGPD:

1.- **Mecanismos de certificación, y de sellos y marcas de protección de datos,** que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes. Para su obtención, se deberán seguir las directrices o criterios que los Estados de la Unión determinen para la aplicación de medidas adecuadas y para demostrar el cumplimiento por parte del responsable o del encargado del tratamiento; serán expedidas por los organismos de certificación[1] o

[1] La AEPD entiende que, de entre estas posibilidades, la que mejor responderá a las necesidades de las entidades al tiempo que es compatible con la configuración y posibilidades de actuación de la Agencia es la de encomendar la certificación a entidades especializadas debidamente acreditadas y dejar que se ocupe de la acreditación de éstas la Entidad Nacional de Acreditación (ENAC), contando para ello con la participación de la Agencia.

por la autoridad de control competente, sobre la base de los criterios que sean aprobados por dicha autoridad (en nuestro país, la Agencia Española de Protección de Datos).

En este caso, los responsables o encargados que quieran someter su tratamiento al mecanismo de certificación deberán dar al organismo de certificación, toda la información y acceso a sus actividades de tratamiento que necesiten para llevar a cabo el procedimiento de certificación.

La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada siempre y cuando se sigan cumpliendo los requisitos pertinentes.

2.- **Códigos de conducta**: El nuevo RGPD permite elaborar códigos de conducta tanto a las instituciones oficiales pertinentes como a Asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento, para contribuir a la correcta aplicación del Reglamento, teniendo en cuenta las características específicas de los distintos tipos de empresas en cuanto a su sector y tamaño. Dichos códigos de conducta deberán contener los mecanismos necesarios para efectuar el control de cumplimiento por los responsables o encargados de tratamiento que se adhieran y comprometan a aplicarlo.

Para la aceptación de un nuevo código de conducta, modificación o ampliación de uno existente la autoridad de control se encargará de evaluar y, en su caso, dictaminar conforme al nuevo Reglamento. Una vez aprobados, serán publicados y registrados por la AEPD para demostrar la existencia de las garantías que persigue el Reglamento para la protección de los derechos de los interesados.

La adopción o adhesión a dichos mecanismos de "prueba del cumplimiento" son de carácter voluntario; no obstante, no limitarán la responsabilidad del responsable o encargado del tratamiento y se entenderán sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes.

Febrero de 2018

C/ Velázquez, 78 - 1º
28001 - Madrid
T +34 911 433 038
F +34 917 915 674
info@lifeabogados.com

lifeabogados.com

A CORUÑA
MADRID
LIMA