PRINCIPALES NOVEDADES DEL RGPD. DECÁLOGO PARA EL CUMPLIMIENTO

Septiembre de 2017

DECÁLOGO PARA EL CUMPLIMIENTO RGPD

1.- El más importante, principio de "**responsabilidad proactiva":** 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 y a partir de este conocimiento determinar de forma clara la manera en que aplicarán las medidas de seguridad más adecuadas y acordes con el tamaño y estructura de la organización para **cumplir** con el RGPD y estar en condiciones de poder **demostrarlo** tanto ante los propios interesados (personas físicas) como ante las autoridades de supervisión (agencia española de protección de datos).

Por tanto ya no se contempla un 'listado o catálogo' de medidas de seguridad a implantar - como se regula en el actual Reglamento de desarrollo de la LOPD (medidas de nivel bajo/medio/alto), sino que es la propia organización quien deberá definirlas, **en atención al riesgo** del tratamiento para los derechos y libertades de las personas. Esto implica **hacer un análisis del flujo de datos (data mapping), de los riesgos para la privacidad, y de la legitimidad del tratamiento.**

Las grandes organizaciones, como regla general, deberán efectuar un análisis de riesgos utilizando alguna de las metodologías de análisis de riesgo existentes.

2.- En el supuesto de que el tratamiento de datos pueda entrañar un **alto riesgo** para los derechos y libertades de los interesados, en estos casos – y con carácter previo a la puesta en marcha de dicho tratamiento- la Empresa deberá realizar una **Evaluación de Impacto sobre la Protección de Datos (EIPD).**

Se considera que los tratamientos conllevan un alto riesgo, los siguientes:

- 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.
- Observación sistemática a gran escala de una zona de acceso público.

Igualmente, se deberá tener en cuenta:

- ✓ El número de interesados afectados.
- ✓ 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.

3.- Protección de Datos desde el Diseño y por Defecto: las empresas deberán -con anterioridad al tratamiento de datos- tomar medidas organizativas y técnicas para integrar en los tratamientos **garantías** que permitan aplicar de forma efectiva los principios del RGPD y que solo se traten los **datos mínimos, necesarios** para la/s finalidad legitima perseguida.

4.- Ya no se permite el **consentimiento** tácito para el tratamiento de los datos (mediante casillas pre marcadas, silencio, etc.), debe ser **inequívoco** y en algunos casos **explícito** (categorías especiales de datos). Esto conlleva revisar cual es la **base jurídica del tratamiento/s que realizamos, y en el supuesto de que se base en el consentimiento, cómo hemos procedido a su recogida.**

Así pues, los tratamientos de datos iniciados con anterioridad al inicio de la aplicación del RGPD (mayo 2018) sobre la base del consentimiento solo seguirán siendo legítimos si ese consentimiento se hubiera prestado del modo en que prevé el propio RGPD, es decir, mediante una manifestación o acción afirmativa. En otro caso habrá que valorar si existe otra base legal que lo legitime.

En el caso de **menores**: El RGPD prevé que el consentimiento solo será válido a partir de los 16 años, debiendo contar en otro caso con la autorización de los padres o tutores legales. Se permite a los estados miembros establecer una edad inferior, siempre que no sea menor de 13 años. En el caso de España, actualmente –hoy por hoy- el consentimiento de los menores es válido a partir de los **14 años.**

5.- **Información y derechos**: la **información** que hay que ofrecer a los interesados en el momento en que se soliciten los datos es **más amplia** y debe proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo (evitando términos vagos, cláusulas farragosas, lenguaje retórico, etc.). Ello implica **revisar y modificar las cláusulas y leyendas informativas que hasta la fecha venimos utilizando en la empresa** con anterioridad a mayo de 2018. Desde las Autoridades de Protección de Datos se recomienda adoptar un modelo de información por capas o niveles.

El RGPD contiene los ya tradicionales **derechos** ARCO y también algunos nuevos, y establece condiciones concretas sobre el procedimiento a seguir para atender a los interesados en el ejercicio de sus derechos. Por tanto debemos **revisar los mecanismos que ofrecemos para el ejercicio de derechos** y **procedimientos con que contamos**, que sean sencillos, claros, permitan verificar la identidad de quien los ejerce, responder en plazo, atender las peticiones de nuevos Derechos, si contamos o no con la colaboración del Encargado para su respuesta, etc.

6.- Outsourcing/Encargados del tratamiento (prestación de servicios por terceras entidades con acceso a datos personales de la Empresa): Las empresas habrán de elegir únicamente encargados/proveedores 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. **La empresa podrá incurrir en responsabilidades por falta de diligencia en la elección del proveedor**.

La relación jurídica responsable-encargado debe formalizarse en un **contrato**, exigiendo el RGPD un contenido mínimo. Por ello, **los contratos de encargo efectuados con anterioridad a la aplicación del RGPD en mayo de 2018 deben modificarse y adaptarse para respetar ese contenido.**

7.- Registro de operaciones de tratamiento: responsables y proveedores (encargados del tratamiento) con más de 250 empleados, deberán mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el RGPD (como por ej. Nombre y datos de contacto del responsable o corresponsable y 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…).

La Agencia Española de Protección de Datos (AEPD) con la finalidad de facilitar la constitución de estos registros, permitirá, 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 a partir del cual realizar y mantener el documento de registro de operaciones.

8.- Las empresas, deberán **notificar a la Agencia Española de Protección de datos, las violaciones o quiebras de seguridad** de los datos que supongan un riesgo para los derechos y libertades de los afectados y en caso de que entrañe un alto riesgo, se notificará también a los **propios interesados**. **Hay que habilitar en la empresa protocolos y procedimientos de actuación, documentación y notificación.**

9.- Se establece la obligación de designar por las empresas un **Delegado de Protección de Datos (DPD),** cuando se traten de

- Autoridades y organismos públicos
- Que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala
- 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. Pudiendo ser interno o externo.

10.- Transferencia internacional de datos fuera de la UE: Se siguen los **mismos criterios** actuales, pero se amplía la lista de posibles instrumentos para ofrecer garantías. Excepción: satisfacer intereses legítimos (debiendo concurrir determinadas circunstancias).

Las decisiones de adecuación, cláusulas tipo contractuales y autorizaciones de transferencias adoptadas y otorgadas por la Comisión con anterioridad a la aplicación del RGPD seguirán siendo válidas, en tanto no se sustituyan, deroguen o 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 proveedor (encargado de tratamiento).

Madrid, septiembre de 2017

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