COMPROMISO
nueva economía
empatía
GLOBALIDAD
TRANSPARENCIA
profesionalidad
método
Comunidad
honestidad
tecnología
Modernidad
Avanzar
Corazón
Innovación
TRANSPARENCIA
Construir
éxito.

CÓMO ADAPTAR NUESTRA ORGANIZACIÓN AL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

¿CÓMO AFECTA A MI ORGANIZACIÓN EL NUEVO REGLAMENTO DE PROTECCIÓN DE DATOS (UE) 2016/679 DE 27 DE ABRIL DE 2016? ¿A QUÉ NOS OBLIGA? ¿CÓMO ADAPTARNOS A LA NUEVA REGULACIÓN?

El Reglamento General de Protección de Datos (en adelante, El Reglamento o RGPD) ha entrado en vigor el 25 de mayo de 2016, y **es de directa aplicación a partir del 25 de mayo de 2018**. Pese a este, aparente, largo plazo interino, ya ha transcurrido casi un año desde su publicación y los profesionales y organizaciones no podemos esperar hasta el mismo día de su obligado cumplimiento para reaccionar, sino que debemos **anticiparnos,** ir dando cumplimiento a las obligaciones que en él se contienen, y así estar preparados para cuando llegue ese momento:

Entonces **¿debemos hacer algo antes de su aplicación, el próximo 25 de mayo de 2018?** La respuesta, y nuestro consejo, es **Si,** como ya ha tenido ocasión de pronunciarse la Agencia Española de Protección de Datos: "*Precisamente el periodo de dos años hasta la aplicación del Reglamento tiene como objetivo permitir que los Estados de la Unión Europea, las Instituciones Europeas y también* ***las organizaciones que tratan datos vayan preparándose y adaptándose para el momento en que el Reglamento sea aplicable***" (más info, "El Reglamento de protección de datos en 12 preguntas" AEPD)

CON ESTA CIRCULAR PRETENDEMOS RESUMIR LOS ASPECTOS MAS RELEVANTES DEL NUEVO REGLAMENTO, SUS PRINCIPIOS, Y MEDIDAS QUE DEBEN SER ADOPTADAS PARA SU CUMPLIMIENTO.

1.- RESUMEN PREVIO:

1º.- Ya no será suficiente adoptar una serie de medidas, sino que debemos estar en condiciones de **poder demostrar que esas medidas cumplen con el Reglamento y son verdaderamente eficaces** (responsabilidad proactiva)

2º.- Ya no es posible tratar datos bajo la fórmula del consentimiento tácito (silencio, casillas ya marcadas, inacción del afectado). **Se requiere una manifestación de voluntad inequívoca y para cada uno de los fines del tratamiento**.

3º.- Si se pretende realizar un **tratamiento ulterior para un fin distinto**, que no sea aquel para el que se recogieron los datos, **se deberá previamente informar al interesado**.

4º.- Por "**defecto**", tan solo podrán recogerse y tratarse los datos que sean **estrictamente necesarios para el cumplimiento de los fines perseguidos** en su recogida y tratamiento.

5º.- Las medidas técnicas y organizativas a adoptar ya no se clasifican por niveles de seguridad, sino que será el Responsable del tratamiento quien "**diseñe**" las mismas en atención al estado de la técnica, coste, tipo de datos, naturaleza, ámbito, contexto y fines del tratamiento y los **riesgos** concretos que en su actividad y organización puedan existir para los derechos y libertades de las personas.

6º.- La Empresa deberá contar con un **registro de las actividades de tratamiento.**

7º.- En el supuesto de que el tratamiento **entrañe un elevado riesgo** para los derechos y libertades de las personas, y en determinados supuestos (tratamientos a gran escala, elaboración de perfiles –automatizado-, etc.), será obligatorio realizar una **evaluación de impacto** antes de iniciar el tratamiento

8º.- Obligatoriedad en determinados supuestos de designar y contar con los servicios de un **Delegado de Protección de Datos o DPO** (Data Protection Officer)

2.- PRINCIPIOS ESENCIALES

2.1.- Principio de Responsabilidad Proactiva: ¿qué significa, qué implica?

El RGPD lo describe como *la obligatoriedad de que el responsable del tratamiento trate los datos y aplique las medidas técnicas y organizativas apropiadas, a fin de garantizar y **poder demostrar** que el tratamiento es conforme y cumple con los principios, derechos y garantías que el Reglamento establece.*

Por tanto, las empresas serán responsables de que los datos sean: (i) tratados de manera lícita, leal y transparente; (ii) recogidos con arreglo a fines determinados, explícitos y legítimos, conforme a los cuales serán tratados; (iii) recopilados de forma adecuada, pertinente y limitada a lo necesario, en relación a tales fines; (iv) exactos y

actualizados si fuera necesario, (v) conservados durante no más tiempo del necesario; y (vi) tratados de tal manera que se garantice su seguridad.

Una actitud "proactiva" exige **diligencia, atención**; y si la proactividad viene a predicarse o define a **aquellas personas con iniciativa y capacidad para anticiparse a problemas o necesidades futuras**, también podríamos decir que la aplicación práctica de **este principio conlleva que debamos tomar el control, prevenir e ir por delante en el análisis y adopción de las medidas que nos permitan cumplir con las exigencias del RGPD, ser capaces de poder demostrarlo y por tanto, estar listos al momento de su obligada aplicación.**

Para ello contamos "aparentemente" con un largo periodo de tiempo (2 años); aparente, en la medida en que **todo proceso de diagnostico y adaptación exige y requiere su tiempo.** Y en palabras del poeta Virgilio, ***tempus fugit***.

2.2.- Protección de datos desde el diseño y por defecto: ¿A qué obliga?

Las empresas deben evaluar y tener en cuenta qué **tipo** de datos tratan, con qué y para qué **finalidades** lo hacen, qué **operaciones** de tratamiento realizan, así como los ***riesgos*** de distinta probabilidad y gravedad que dichos tratamientos comporten para los derechos y libertades de las personas físicas, a fin de adoptar las ***medidas apropiadas*** que cumplan con el Reglamento (teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse), y garantizar que solo serán objeto de tratamiento los ***datos necesarios*** para cada uno de los fines previstos.

Dichas medidas podrían consistir, entre otras en:

- Seudonimizar los datos personales
- Cifrado
- Minimizar, reducir al máximo el tratamiento de datos personales
- Transparencia en la información
- Permitir a los interesados supervisar el tratamiento de datos
- Limitar el tratamiento
- Garantías de la seguridad

No olvidemos, como ya hemos indicado (responsabilidad proactiva), que **hay que poder demostrar su cumplimiento** ante los propios interesados[1], afectados por el tratamiento, y las autoridades de control y supervisión. **No cabe la improvisación**.

[1] [1] "Interesado": toda información sobre una persona física identificada o identificable.

3.- PROCESO DE ADAPTACIÓN: CRITERIOS Y PASOS A SEGUIR.

3.1. ¿Cómo actuar, qué recomienda la Agencia Española de Protección de Datos?

Recientemente la Agencia Española de Protección de Datos (AEPD), ha publicado nuevos materiales para ayudar a las pymes a cumplir con el Reglamento europeo y facilitar que, en este periodo transitorio, las pymes conozcan el impacto que va a tener el Reglamento en la forma en la que tratan datos y las medidas a adoptar: en algunos casos, las recomendaciones o interpretaciones que se ofrecen en las Guías 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 (por ejemplo, el modo de obtención del consentimiento); en otros, esas recomendaciones o propuestas solo deberán tenerse en cuenta en el momento en que el RGPD sea de aplicación. (Vid. http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_01_26_01-ides-idphp.php).

En el Despacho **LIFE Abogados**, en consonancia con las recomendaciones de la AEPD, hemos diseñado un **modelo de adaptación de las empresas y organizaciones al nuevo marco regulador de la protección de datos,** mediante: (i) el análisis y evaluación de impacto del nuevo RGPD; (ii) propuesta de medidas correctoras o a implantar; (iii) modelos, y (iv) plazos de puesta en práctica.

No todas las compañías deberán cumplir en igual medida las exigencias del Reglamento, pero si todas deberán estar en condiciones de poder *demostrar su idoneidad, eficacia y cumplimiento*.

3.2. Criterios (análisis RGPD) y pasos a seguir

a) **Enfoque de riesgo:** las medidas dirigidas a garantizar el cumplimiento del RGPD deberán 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. Un análisis y clasificación de estos riesgos, permitirá: i) determinar las **medidas de seguridad más adecuadas en atención al mayor o menor nivel de riesgo** que presente el tratamiento de los datos, y ii) **garantizar** que se cumpla con el Reglamento y la protección de los derechos de los interesados.

"Identificable": toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

En consecuencia, las medidas previstas en el RGPD deberán adaptarse y tener en cuenta **las características específicas de la empresa y el tipo de tratamientos llevados a cabo por la misma**.

Lo que puede ser adecuado para una organización que maneja datos de muchos miles de personas, en tratamientos complejos, que conlleven 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 o en pequeña escala.

b) **Evaluaciones de impacto de las operaciones de tratamiento,** cuando sea probable que un tipo de tratamiento entrañe un **alto riesgo** para los derechos y libertades de las personas físicas. Particularmente y con carácter previo, cuando se realicen determinados tratamientos:

- Elaboración de perfiles
- Tratamiento a gran escala (datos salud, ideología, origen racial, condenas, infracciones penales, etc.)
- Observación sistemática a gran escala de una zona de acceso público

La AEPD considera que no debería esperarse a la fecha de aplicación del Reglamento para comenzar a utilizar esta herramienta, ya que **requiere de una preparación, metodología y equipo de trabajo que no pueden improvisarse**.

c) **Consentimiento**: las personas cuyos datos se traten deben prestar su consentimiento mediante una **manifestación inequívoca o una clara acción afirmativa**. No podrá utilizarse ya la fórmula actual del llamado *consentimiento tácito,* por defecto: el silencio, las casillas ya marcadas o la inacción no deben validar el consentimiento.

Por tanto, a partir de mayo de 2018, sólo serán válidos los tratamientos basados en el consentimiento inequívoco, con independencia de cuándo se haya obtenido ese consentimiento. Y el responsable deberá ser capaz de **demostrar** el consentimiento prestado por los interesados.

d) **Transparencia de la Información:** el RGPD regula un derecho de información **más amplio,** con supuestos no requeridos por la actual normativa (vgr. fines y base jurídica del tratamiento, plazo de conservación de los datos, datos contacto del Delegado de Protección de datos en su caso, existencia de decisiones automatizadas, derecho a la portabilidad de los datos).

Las empresas y organizaciones hemos de aprovechar estos meses para realizar una **adaptación progresiva de las leyendas y clausulas informativas** que se vienen utilizando, actualizándolas, generando nuevas políticas y modelos de información, y **hacer llegar progresivamente a los clientes y usuarios la información adicional,** y completa, a través de medios electrónicos (páginas Web, e-mail) o canales habituales de comunicación con los clientes.

La información a suministrar deberá ser de **transparente, concisa, inteligible y de fácil acceso,** utilizando un **lenguaje claro y sencillo.**

e) **Designación de un Delegado de Protección de Datos** (DPD/DPO -*Data Protection Officer*-): EL RGPD establece la **obligación** de designar a un DPO en determinados supuestos, y contar con la ayuda y asistencia de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos, que puede ser de la plantilla, o contratado en régimen de prestación de servicios por el responsable o encargado del tratamiento y a quien se le dotará de los **recursos necesarios** para el desempeño de sus funciones, y en condiciones de poder desempeñar sus funciones y cometidos de manera **independiente.**

- ✓ En el *sector público* es en todo caso obligatorio la figura del DPO.

- ✓ En el *sector privado* será obligatorio si:

  - Las actividades principales consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados.
  - Si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales (salud, religión, ideología, etc.) y de datos relativos a condenas e infracciones penales.

Además, se establece que **los interesados podrán ponerse en contacto con el DPO** por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento. Por ello, las **empresas** (responsables o encargadas del tratamiento) deberán **hacer públicos los datos de contacto del DPO** y lo comunicarán a la autoridad de control.

f) **Códigos de conducta y Certificaciones:**

Si bien los códigos de conducta ya vienen regulados en la LOPD 15/1999, el Reglamento europeo viene a reforzar y regular estas figuras como herramientas idóneas para: (i) facilitar a las Empresas, Asociaciones y organismos representativos de categorías de responsables o encargados del tratamiento, incluidas las Administraciones Públicas, la correcta aplicación del RGPD; (ii) demostrar el cumplimiento del RGPD; (iii) evaluar el impacto y efectos en protección de datos de las operaciones de tratamiento; y (iv) proporcionar garantías adecuadas en el caso de transferencias internacionales de datos.

En definitiva, la adhesión a códigos de conducta o contar con una certificación, sello o marca en protección de datos, **permitirá evaluar** con mayor rapidez a las empresas el nivel de protección de los datos y cumplimiento de las obligaciones sobre medidas de seguridad, en atención a las características y necesidades particulares de los distintos sectores de actividad.

La adhesión a códigos de conducta o mecanismos de certificación (de carácter voluntario) **será tenida en cuenta en procedimientos sancionadores** a la hora de evaluar la multa (oscilan entre 10 y 20 millones de euros o el 2 o 4% del volumen de negocio total anual global).

g) **Comunicación de violación de la seguridad de los datos a la autoridad de control y al propio interesado:** Esta es una importante novedad que introduce el RGPD.

Hasta ahora no era obligatorio informar a las autoridades cuando se producía una transgresión de la seguridad de los datos, pero el nuevo Reglamento regula un sistema de **notificaciones obligatorio** para las Empresas, que deberán efectuarse:

- sin dilación indebida
- si es posible, a más tardar en 72 horas
- descripción de su naturaleza, alcance, medidas adoptadas…

Esta obligación **será eludible** si el responsable puede demostrar la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

Cuando sea probable que la violación entrañe un **alto riesgo** para los derechos y libertades de las personas se comunicará así mismo al interesado/s, en un lenguaje claro y sencillo.

Esta obligación también recae sobre el **encargado del tratamiento**, que deberá igualmente notificar al Responsable cualquier violación de la seguridad de la que tenga conocimiento.

EN CONCLUSIÓN: la recomendación es comenzar paulatina y progresivamente a incorporar la nueva regulación en protección de datos, lo que no solo permitirá a las empresas y organizaciones estar en condiciones de **asegurar su cumplimiento** cuando llegue el momento en que ya sea obligatorio, sino también la **continuidad sin sobresaltos de la buena marcha del negocio y actividad de la empresa**.

En el Despacho **LIFE Abogados** contamos con un departamento especializado en estas áreas del Derecho, y estamos en las mejores condiciones para prestarles asesoramiento en esta materia.

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