CIRCULAR INFORMATIVA SOBRE EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS (RGPD)

"De la LOPD al RGPD, una transición obligada"

Estimado asesor/a:

Como ya sabréis, el 25 de mayo de este año será el último día para comenzar con la aplicación del nuevo Reglamento Europeo 679/2016 de Protección de Datos o RGPD, que entró en vigor el pasado 25 de mayo de 2016.

Este nuevo Reglamento trae consigo los cambios más importantes que se han producido en materia de protección de datos en los últimos años, con la firme intención de homogeneizar todas las normativas vigentes en los Estados Miembros que componen la Unión Europea y con el objetivo de ampliar las garantías de control que sobre sus datos tienen los ciudadanos.

Sin embargo, la falta de información y de definición por parte de las autoridades nacionales ha generado cierta incertidumbre entre las empresas sobre cómo aplicar la nueva normativa.

En paralelo a la aplicación del RGPD a nivel europeo, el Ministerio de Justicia ha aprobado un anteproyecto de nueva "LOPD" que complementa y aclara algunos aspectos del RGPD, pero todavía no la tenemos disponible, de hecho aún está pendiente de aprobación definitiva, estando actualmente en el último trámite parlamentario para su publicación y entrada en vigor.

No obstante, y debido a que, probablemente la nueva LOPD se aprobará el mismo día que entre en vigor el nuevo Reglamento, hace tiempo que venimos analizando el nuevo reglamento europeo de protección de datos y sí podemos destacar sus aspectos más relevantes, así como aquellos que pueden afectar a nuestro servicio de consultoría.

Hemos trabajado en las nuevas obligaciones y hemos dejado nuestros servicios de consultoría preparados para que antes de mayo de 2018 tu despacho profesional cumpla al 100% con el RGPD.

1) ¿Va a suponer más carga de trabajo para las empresa aplicar el RGPD?

NO, aunque si bien el Reglamento va a suponer mayor compromiso por parte de las empresas con la protección de datos, esto no se traducirá necesariamente en una mayor carga de trabajo.

Y es que, si partimos de la base de que actualmente ya llevamos una correcta gestión de la LOPD, podemos considerar la adaptación al RGPD como una continuación de las medidas que ya estamos aplicando.

2) Nueva forma de obtener el consentimiento.

Podemos decir que es uno de los cambios más importantes del RGPD, ya que si hasta ahora teníamos varias formas de obtener el consentimiento para el tratamiento de datos, el RGPD establece que solamente se podrá obtener con una declaración clara de los interesados o una acción positiva que indique el acuerdo del mismo, es decir, el consentimiento debe ser expreso. Se prohíben, por tanto, prácticas como el consentimiento tácito o por omisión.

Desde nuestro departamento técnico ya se han elaborado las nuevas cláusulas para obtener el consentimiento conforme al RGPD.

3) Nuevas cláusulas de información.

Las actuales cláusulas informativas y avisos legales, deberán de ser revisadas y actualizadas. El RGPD prevé que se incluya en la información que se proporciona a los interesados, una serie de cuestiones que, con la Directiva del año 95 y muchas leyes nacionales de transposición, no eran necesariamente obligatorias, como por ejemplo la base jurídica del tratamiento, el plazo de conservación de los datos o los criterios para su determinación.

Esta información deberá proporcionarse de forma concisa, transparente, inteligible, de fácil acceso, con un lenguaje claro y sencillo, por escrito u otros medios y de forma gratuita.

Igualmente pondremos a tu disposición dichos avisos legales donde se cumple con el deber de informar conforme al RGPD.

4) Nuevos contratos con terceros. Los Encargados de Tratamiento.

Este punto tiene especial incidencia para ti como asesor o gestor, ya que es uno de aspectos que sufre más cambios, tanto para los responsables como para los encargados del tratamiento. Esto significa que se tendrán que revisar y actualizar los anteriores contratos de acceso a los datos por cuenta de terceros del Art. 12 de la LOPD, y sustituirlos por los nuevos contratos entre el responsable y el encargado del tratamiento.

Este nuevo contrato se amplía en su contenido y necesariamente deberán incluir entre otros aspectos: descripción detallada de los servicios prestados y la naturaleza o finalidad del tratamiento,medidas aplicadas, la duración, el tipo de datos personales y categorías de interesados, así como las obligaciones y derechos del responsable posibles transferencias internacionales de datos, subcontrataciones previstas, qué pasa cuando se finaliza el tratamiento, etc.

Por lo que será obligatorio volver a firmar con todos los terceros los nuevos contratos adaptados al RGPD.

Dicho contrato ya está redactado por nuestros consultores y se te facilitará desde nuestro departamento de consultoría.

5) Niveles de seguridad de los datos.

Los niveles de los datos dejan de diferenciarse, como hasta ahora, en básico, medio, alto, para aplicar las correspondientes medidas de seguridad, pasando a clasificarse simplemente como datos SENSIBLES y NO SENSIBLES. Además, el RGPD incluye en los datos SENSIBLES, dos nuevas categorías en este apartado: datos genéticos y datos biométricos.

6) Cambios en las medidas de seguridad.

Ya no se establecen medidas de seguridad específicas, tal como se contemplaban en el R.D. 1720/2007, sin embargo, aparece el concepto de RESPONSABILIDAD PROACTIVA (accountability), que hace referencia a la prevención por parte de las organizaciones que tratan datos.

Es decir, las empresas, deberán aplicar las medidas necesarias que garanticen criterios de seguridad como: confidencialidad, integridad, disponibilidad y resiliencia.

¿Cuáles son estas medidas de seguridad PROACTIVAS?:

- Protección de datos desde el diseño (PDdD).
- Protección de datos por defecto (PDpD).
- Medidas de seguridad (técnico-organizativas).
- Mantenimiento de un registro de actividades de tratamiento. (se desarrolla más abajo)
- Análisis de riesgos y evaluaciones de impacto (cuando sea probable que el tratamiento presente un alto riesgo específico para los derechos y libertades de los interesados).
- Nombramiento de un delegado de protección de datos (DPO) (solo en determinados supuestos).
- Notificación de violaciones de la seguridad de los datos, o brechas de seguridad.

7) Registro de ficheros

La actual inscripción de ficheros ante la Agencia de Protección de Datos (AEPD) desaparece como tal, sin embargo se obliga al responsable de tratamiento (RT) y al encargado de tratamiento (ET) a llevar un "registro de actividades de tratamiento" con un contenido mínimo que, de algún modo, sería el equivalente a nuestro actual "Documento de Seguridad".

8) Derecho al olvido y Derecho de portabilidad

Además de los ya conocidos derechos ARCO (acceso, rectificación, cancelación y oposición), el RGPD introduce nuevos conceptos como el derecho al olvido (manifestación de los tradicionales derechos de cancelación y oposición aplicados a los buscadores de internet) y derecho a la portabilidad (permite al interesado recuperar sus datos de forma estructurada para trasladarlos a otro responsable).

9) Delegado de Protección de Datos (DPD)

Este concepto ha generado mucho ruido entre las empresas pero parece que todavía no está claro quién tendrá la obligación de nombrar a esta figura y para quién quedaría como una simple recomendación en función del tipo de datos personales que se traten influyendo por el tamaño de la empresa o el volumen de datos tratados.

Se tendrá que designar un delegado de protección de datos siempre que;

- el tratamiento lo lleve a cabo una **autoridad u organismo público** (excepto tribunales cuando actúen en su función jurisdiccional).
- las actividades principales consistan en operaciones que requieran una **observación habitual y sistemática de interesados a gran escala.**
- las actividades principales consistan en el **tratamiento a gran escala de categorías especiales de datos personales.**

Desde nuestra entidad realizaremos un análisis de riesgo previo para evaluar cada entidad y determinar la necesidad de nombrar un Delegado de Protección de Datos.

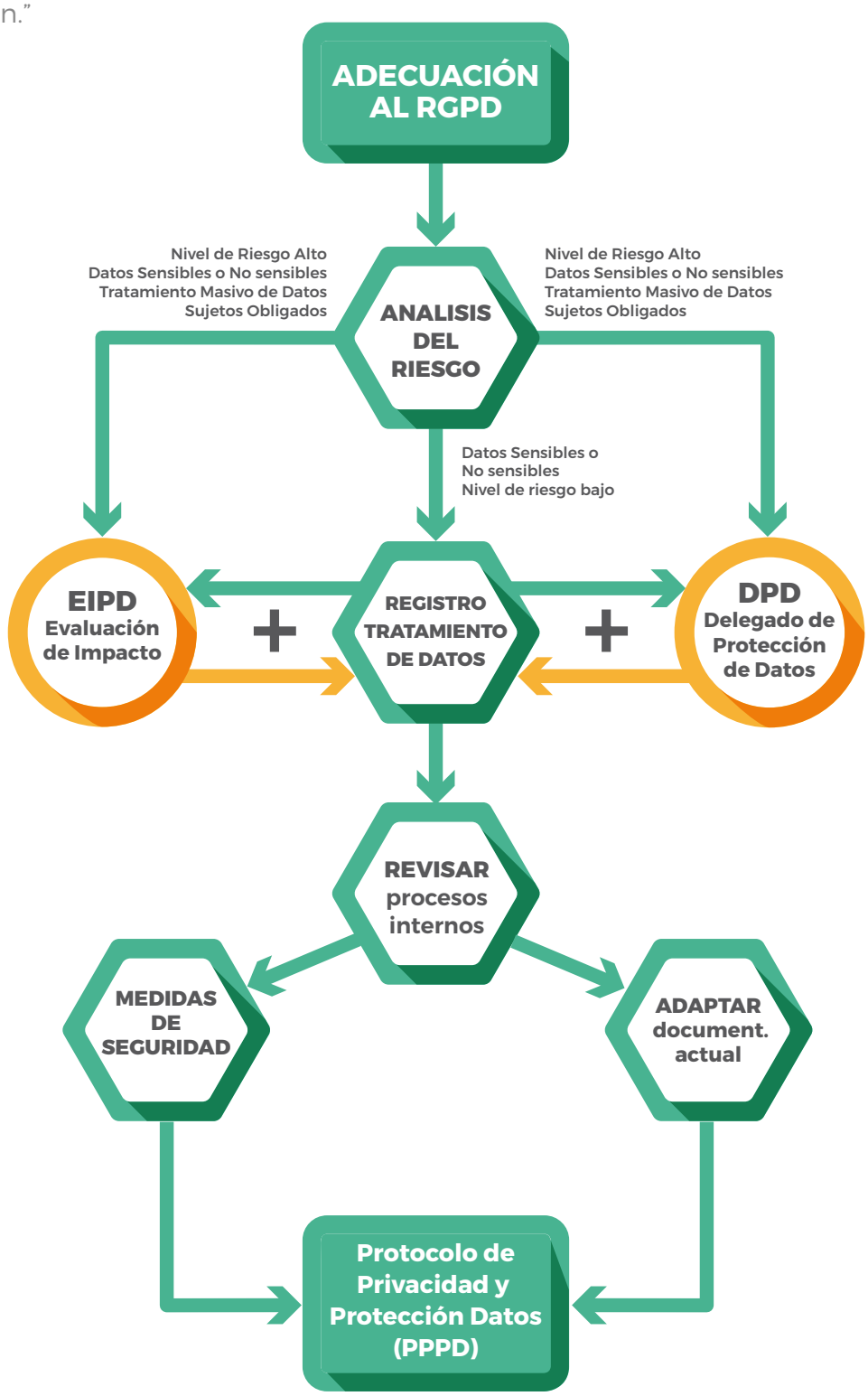
El DPD será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados en Derecho y la práctica en materia de protección de datos. Podrá formar parte de la plantilla de la entidad **o realizar sus funciones como externo mediante un contrato de prestación de servicios. En los próximos meses le iremos informando sobre la posibilidad de que nuestra entidad sea el DPD de su despacho profesional o de sus clientes.**

10) Evaluación de Impacto (EIPD)

Es otra de las novedades que trae consigo el RGPD y podemos definirla como un análisis de los riesgos que un producto o servicio puede entrañar para la protección de datos de los afectados y, como consecuencia de ese análisis, la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos.

Al igual que la valoración sobre la obligatoriedad de tener un DPD, desde nuestra entidad se evaluará en base al análisis de riesgo previo si tu asesoría precisa de la realización de esta evaluación de impacto para la privacidad.

Conclusión

"Resulta evidente que hoy día, **la correcta implantación y cumplimiento de la normativa en materia de protección de datos** ya no va a depender de formales obligaciones e inamovibles

medidas de seguridad y protocolos, sino que se **requerirá de una constante proactividad e implicación por parte del responsable del fichero que conlleva necesariamente un asesoramiento inmediato y constante, como por ejemplo;** en el desarrollo de nuevas vías de negocio, cuando haya posibles conflictos o brechas de seguridad, que afecten a la privacidad y a los datos personales, ante posibles denuncias, ante peticiones de terceras personas, o bien en aquellas situaciones en las que los gerentes o responsables de seguridad piensen que pueda tener relación."