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

"De la LOPD al RGPD, una transición obligada"

El pasado 25 de mayo comenzó la aplicación efectiva del nuevo Reglamento Europeo 679/2016 de Protección de Datos o RGPD.

El Ministerio de Justicia aprobó un anteproyecto de nueva "LOPD" que complementa y aclara algunos aspectos del RGPD, pero todavía está en el último trámite parlamentario para su publicación y entrada en vigor. Esto está provocando mucha confusión a la hora de aplicar la nueva normativa, generando situaciones como, por ejemplo, plantear que un Asesor Fiscal tiene que tener un DPO (o DPD - Delegado de Protección de Datos) o que tenga que hacer una evaluación de impacto.

Ante tanta confusión y la eminente entrada en vigor del RGPD, vamos a intentar aclarar algunos conceptos, obligaciones y, sobre todo, transmitir la calma necesaria para contratar los servicios correctos y aplicar la normativa adecuadamente.

Para ello vamos a empezar por lo que más se habla (DPO y Evaluación de Impacto) y continuaremos con el resto de contenido del RGPD. En cualquier caso, siempre centrándonos en el perfil de un socio de AECE.

1) Delegado de Protección de Datos (DPD o DPO (por sus siglas en inglés))

¡NO!, 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 y donde además influye el tamaño de la empresa o el volumen de datos tratados.
En concreto y a priori, para un Asesor Fiscal, parece que no va a ser obligatorio. En cuanto esté claramente definido por la AGPD y/o en la nueva LOPD, podremos avanzar al respecto.

Cuando hablamos de "a priori" es porque nos basamos en los criterios consignados en el RGPD para determinar la obligatoriedad del DPD. En concreto son:

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.**

Sin entrar en grandes detalles con respecto a la "laguna legal" que hay en este tema, solo habría que hacerse una pregunta: ¿qué es gran escala? 1.000 datos, 10.000 clientes, 100.000 pacientes...

Por lo tanto, ¡Ojo! con contratar un servicio de DPD que puede no ser ni obligatorio, ni necesario.

2) Evaluación de Impacto

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. Nos gustaría basarnos en la nueva LOPD para determinar esta obligación con más certeza, pero antes esa falta usaremos nuestros 15 años de experiencia en asesoramiento de protección datos.

3) 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.

Nuestro departamento de consultoría ya ha elaborado las nuevas cláusulas para obtener el consentimiento conforme al RGPD.

4) 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 1995 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, nuestros clientes tienen a su disposición dichos avisos legales donde se cumple con el deber de informar conforme al RGPD.

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

Este punto tiene especial incidencia para ti como asesor o gestor, ya que es uno de los 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: una 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, obligaciones y derechos del responsable, posibles transferencias internacionales de datos, subcontrataciones previstas, qué ocurre con los datos 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 nuestro departamento de consultoría y a disposición de nuestros clientes.

6) 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: datos genéticos y datos biométricos.

7) 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. (ver página siguiente)
- 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.

8) 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".

9) 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).

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."

Departamento de Consultoría
Telf.: 958 415 736
Email: info@grupoiwi.com
Web: www.grupoiwi.com