REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS: EL NUEVO MARCO NORMATIVO EUROPEO EN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Mayo 2016

Estimados Sres.:

Tras un largo proceso legislativo de más de 4 años, el pasado 4 de mayo de 2016 se ha publicado en el Diario Oficial de la Unión Europea el **Reglamento General de Protección de Datos** (en adelante, el "**RGPD**") recientemente aprobado por el Pleno del Parlamento Europeo y que, tras su entrada en vigor, se convertirá en la nueva normativa de referencia en materia de protección de datos en la Unión Europea (en adelante, la "**U.E.**").

Dicho texto, que **resultará de aplicación directa en los Estados miembros de la U.E.,** persigue, entre otras finalidades, (i) **eliminar cargas burocráticas** relacionadas con la protección de datos; (ii) **armonizar la normativa aplicable en los diferentes Estados miembros** eliminando las diferencias actualmente existentes; y (iii) en suma, **reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas** en relación con el tratamiento de datos.

La trascendencia del RGPD resulta innegable, en la medida en que su contenido afectará, de forma directa y en diferentes grados según su tipología y actividad, a la organización y al modelo de negocio/actuación de los diferentes operadores incluidos en su ámbito de aplicación (**profesionales, empresas, administraciones públicas y otras entidades del sector público y privado que, en el marco de sus actividades, traten datos de carácter personal**).

Por ello, les remitimos la presente circular, con la intención de hacerles partícipes de los principales aspectos novedosos del RGPD, de cara a facilitarles un primer acercamiento a la materia y esperando que la misma sea de su interés.

BSK
Donostia – San Sebastián ☎ 943 40 00 35
Vitoria – Gasteiz ☎ 945 00 35 35
Pamplona ☎ 948 28 79 99
www.grupobsk.com
bsk@grupobsk.com

GLOBALAW THE INTERNATIONAL LAW GROUP
www.globalaw.net

I. Entrada en vigor y aplicación del Reglamento General de Protección de Datos

El RGPD **entrará en vigor a los 20 días de su publicación en el Diario Oficial de la Unión Europea**, esto es, el próximo 25 de mayo de 2016.

Sin embargo, tal y como dispone el propio RGPD, éste **no será directamente aplicable y, por tanto, no resultará de obligado cumplimiento, hasta el 25 de mayo de 2018** (2 años después de su entrada en vigor).

De este modo, se estaría estableciendo un plazo transitorio que permita a los diferentes operadores afectados por su contenido adaptar progresivamente y según proceda su organización y/o su negocio/actividad a las exigencias previstas en el nuevo marco normativo.

II. Principales novedades introducidas en el Reglamento General de Protección de Datos

A continuación se enumeran, a modo de breve acercamiento a la materia, algunos de los aspectos más relevantes del RGPD y de las novedades normativas que éste incorpora, con especial atención a aquéllas que pudieran resultar más útiles para su actividad:

- **Ámbito de aplicación**

  El RGPD elimina discusiones interpretativas, estableciendo que sus previsiones resultan de aplicación tanto (i) al **tratamiento de datos realizado por un Responsable con establecimiento en la U.E.**; como (ii) al tratamiento de datos de residentes en la U.E. llevado a cabo por **Responsables no establecidos en dicho territorio**, cuando éste tenga por objeto **la oferta de bienes o servicios en la U.E.** o **el control del comportamiento de los interesados en la U.E.** (e.g. archivos cookies u otros dispositivos análogos).

- **Responsabilidad proactiva y la privacidad desde el diseño y por defecto**

  Se amplía el catálogo de **principios aplicables al tratamiento de datos** añadiendo, entre otros, el principio de "**Responsabilidad Proactiva**". Dicho principio, estrechamente relacionado con el concepto anglosajón de "*accountability*", exige al Responsable del Tratamiento que, además de cumplir con todos y cada uno de los principios aplicables, adicionalmente, sea capaz de **demostrar adecuadamente dicho cumplimiento**.

Con carácter complementario, el RGPD introduce dos nuevos conceptos relacionados con los antedichos principios y que resultan de enorme trascendencia:

(i) **la privacidad desde el diseño**, que obliga a tener en cuenta la protección de datos en el momento inicial de la definición de cualquier proceso, producto o servicio; y

(ii) **la privacidad por defecto**, que obliga a que todo tratamiento, conlleve por definición y de forma predeterminada, el estricto cumplimiento de los principios de protección de datos.

- **Nuevos derechos de los interesados**

Al margen de los derechos de acceso, rectificación, cancelación (ahora denominado "*supresión*") y oposición, el RGPD **añade nuevos derechos del interesado**, como (i) el **derecho a la portabilidad de los datos;** y (ii) el **derecho de limitación del tratamiento y el derecho al olvido** (ambos como contenido del derecho de supresión), unificando, asimismo, el procedimiento para el ejercicio de todos los derechos.

- **Sistema de ventanilla única**

Se introduce, asimismo, el sistema denominado de "*ventanilla única*" que permitiría a los interesados cuyos derechos se vean vulnerados presentar su reclamación ante la autoridad nacional de protección de datos correspondiente a su lugar de trabajo o residencia habitual o al lugar donde se hubiera cometido la infracción, con independencia de la sede del Responsable del Tratamiento que hubiera cometido la infracción. A estos efectos se establece una serie de normas procedimentales que regirán la resolución de dicha reclamación.

- **Nuevas obligaciones de información y consentimiento del interesado**

La información que ha de proporcionarse al interesado en el momento en el que se obtengan sus datos se amplía sensiblemente respecto de lo que actualmente establece la **Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal** (en adelante, la "**LOPD**"), previéndose asimismo la posibilidad de utilizar a tal fin iconos normalizados que deberán ser fijados por la Comisión Europea.

Asimismo, **se intensifican los requisitos y condiciones aplicables a la obtención del consentimiento de los interesados**, exigiéndose a tal fin **una declaración o una clara acción afirmativa, sin que la mera inacción pueda interpretarse como consentimiento.** Además, se establece que será necesario el consentimiento del padre/madre o tutor en el caso de los **menores de 16 años.**

- **Inscripción de ficheros y Registro de Actividades de Tratamiento**

  Se elimina la obligación referente a la comunicación/inscripción de ficheros ante las autoridades de control nacionales (en el caso español, la Agencia Española de Protección de datos y las Agencias Vasca y Catalana de Protección de Datos).

  En su lugar, se prevé que **Responsables y Encargados del Tratamiento lleven un Registro de Actividades de Tratamiento**, a modo de registro interno.

- **Medidas de seguridad**

  Se sustituye el catálogo tasado de **medidas de seguridad** obligatorias que, conforme al vigente **Real Decreto 1720/2007, que aprueba el Reglamento de desarrollo de la LOPD** (en adelante, el "**RLOPD**"), habían de ser observadas por el Responsable y el Encargado del Tratamiento, estableciendo en su lugar una **obligación genérica de aplicación de medidas técnicas y organizativas que garanticen un nivel de seguridad adecuado** y unas **categorías mínimas de medidas genéricas**. De esta forma, se estaría otorgando a los operadores una mayor libertad en la definición e implementación de tales medidas.

- **Notificación de violaciones de seguridad**

  Salvo en supuestos excepcionales, los Responsables del Tratamiento tendrán la obligación de **notificar a la autoridad de control competente, en un plazo máximo de 72 horas, toda violación de seguridad de los datos personales**, entendiéndose por tal toda aquélla que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales o la comunicación o acceso no autorizado a los mismos.

  Asimismo, será **necesario notificar a los interesados dicha violación de seguridad, cuando ésta entrañe un alto riesgo para sus derechos y libertades**.

- **La figura del Delegado de Protección de Datos (DPO)**

  El RGPD introduce la figura del **Delegado de Protección de Datos** (DPO, por sus siglas en inglés), atribuyéndole determinadas funciones de información, supervisión y asesoramiento en materia de protección de datos en la organización del Responsable o Encargado del Tratamiento.

  El DPO, que podrá formar parte de la plantilla del operador en cuestión o ser un tercero que presta un servicio externalizado, únicamente se establece **con carácter obligatorio (i) para autoridades u organismos públicos, en todo caso; y (ii) en determinados supuestos tasados para el resto de Responsables o Encargados del Tratamiento (actividades que supongan una observación habitual y sistemática de los interesados o tratamiento a gran escala de categorías especiales de datos personales)**.

- **Evaluaciones de impacto**

  Se impone asimismo que, **con carácter previo al inicio o modificación de determinados tratamientos de datos (en especial para determinadas categorías de tratamientos)**, se elabore, obligatoriamente, una **evaluación de impacto en materia de protección de datos** que, entre otros aspectos, analice la necesidad y proporcionalidad del tratamiento así como los riesgos derivados del mismo, y prevea las medidas y mecanismos que permitan garantizar la protección adecuada de los datos. Dicha obligación habrá de ser debidamente observada para cualesquiera nuevos **procedimientos, productos y servicios** del Responsable del Tratamiento.

- **Normas corporativas vinculantes**

  Se incorporan al texto normativo las normas corporativas vinculantes (conocidas como BCRs por sus siglas en inglés), como mecanismo que permite regular las **transferencias internacionales de datos dentro de un grupo empresarial**, previa su aprobación por la autoridad de control competente (mecanismo que ya se venía aceptando en la práctica).

- **Incremento de la cuantía de las sanciones**

  Por último, el RGPD establece un **incremento significativo de las sanciones aplicables a las infracciones en materia de protección de datos** (multas administrativas), que ahora podrían llegar a alcanzar, según las infracciones de las que se trate, un **importe máximo de 20.000.000 € o un 4% del volumen de negocio total anual, optándose por la mayor de ambas cantidades**. Queda **a disposición de cada estado miembro establecer si las autoridades y organismos públicos de dicho estado pueden ser objeto de multa administrativa y en qué medida**.

III. Régimen transitorio: ¿Qué debemos hacer a partir de ahora?

En primer lugar, es necesario aclarar que durante el período en el que, con el ya aludido carácter transitorio, el RGPD no resulte aun de aplicación, el marco legal actualmente vigente en los estados miembros continuará en vigor.

En el caso de España, como bien conocerán, dicho marco legal está compuesto, en lo fundamental, por la LOPD y el RLOPD.

De este modo, **la entrada en vigor del RGPD no eximirá a profesionales, empresas, Administraciones Públicas y otras entidades de derecho público o privado, del cumplimiento de las obligaciones previstas en la LOPD y en el RLOPD, al menos hasta que se hubiera cumplido el aludido plazo de 2 años**.

Al mismo tiempo, debe tenerse en cuenta que la adaptación a las previsiones del RGPD (muchas de ellas completamente novedosas), requerirá de esfuerzos organizativos, técnicos y humanos de mayor o menor intensidad, según el caso concreto y las actividades de cada operador, y el compromiso e involucración de diferentes estamentos de la entidad en cuestión.

Por ello, las actuaciones comprensivas de la referida adaptación no deberían ser pospuestas hasta 2018, siendo **sumamente recomendable que, en los próximos meses, cada operador y los miembros de su organización valoren la incidencia del RGPD en su organización y en su negocio/actividad, definiendo, en función de dicho análisis, un plan de actuación que permita su progresiva adaptación al nuevo marco normativo**.

IV. Recomendaciones

Atendida la nueva regulación en materia de protección de datos que introduce el RGPD y la trascendencia que la misma está llamada a tener en la organización y desarrollo del negocio/actividades de profesionales, empresas, Administraciones Públicas y otras entidades de derecho público y privado, **debemos recomendarles que tengan en consideración el contenido de la presente circular y que prevean, con la suficiente antelación, la necesidad de proceder a una adaptación tranquila y ordenada a este nuevo marco normativo.**

Por ello, les invitamos a que, en los próximos meses inicien un proceso de reflexión que les permita valorar la incidencia del RGPD en su organización y en su negocio/actividad, definiendo, en función del resultado de dicho análisis, un plan de actuación que permita su progresiva adaptación a las nuevas obligaciones con el alcance que resulte adecuado en atención a las concretas circunstancias de su negocio/actividad.

En este sentido, le anunciamos que, con el fin último de acompañarles en dicho proceso y facilitar su adecuada adaptación al RGPD, **en próximas fechas celebraremos acciones formativas en las que se abordarán con más detalle las principales novedades introducidas por dicho texto normativo.**

Asimismo, queremos indicarles que estamos trabajando en la generación de un **protocolo de actuación que permita identificar de una forma ágil y efectiva las actuaciones a desarrollar, en cada caso, en el marco de la aludida adaptación al RGPD.**

En todo caso, les informaremos debidamente sobre las acciones formativas que desarrollemos y sobre el referido protocolo en una nueva circular.

* * * * *

Queremos advertirles que la presente circular es meramente informativa y, por lo tanto, contiene información de carácter general que no constituye asesoramiento jurídico. En este sentido, si a la vista del contenido del presente documento necesitaran aclarar cualquier aspecto en relación con el contenido del mismo, les rogamos se pongan en contacto con nosotros para que les asesoremos adecuadamente atendiendo a las circunstancias de su caso concreto.

Sin otro particular, les saluda muy atentamente.

BSK LEGAL & FISCAL ASOCIADOS, S.L.P.U.
Departamento de Nuevas Tecnologías
Persona de contacto: Ramón Solórzano
rsolorzano@grupobsk.com