



NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

El 25 de mayo marcará un punto de inflexión en la regulación de la privacidad en toda la Unión Europea. Ha entrado finalmente en vigor-tras un largo y complejo proceso legislativo iniciado en 2012-, el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE*.

Este Reglamento (en adelante, el “RGPD”) es de aplicación directa a los Estados miembros (sin necesidad de trasposición nacional), si bien establece un periodo transitorio para que sea aplicable, a todos los efectos, a partir del 25 de mayo de 2018.

¿Qué se persigue con esta nueva norma?

El legislador europeo ha buscado, con el RGPD:

- 1 Reforzar los derechos de los ciudadanos otorgándoles un mayor grado de control sobre su información privada, a la luz del desarrollo tecnológico de los últimos tiempos y el notable aumento en el tratamiento de datos personales en el mundo digital.
- 2 Aportar mayor seguridad jurídica, estableciendo en toda la UE unos estándares homogéneos de protección de datos personales (adaptados al entorno digital) a través de un marco legal claro y único.
- 3 Reducir de las cargas administrativas de las empresas que traten datos personales.
- 4 Regular el uso de datos para fines judiciales y policiales.
- 5 El cumplimiento estricto de la normativa aplicable, aumentando considerablemente las sanciones en caso de incumplimiento.

Principales novedades y ventajas

1. **Norma única en la Unión Europea, para cualquier empresa europea o extranjera que trate datos personales de ciudadanos europeos.** El RGPD armonizará y unificará las normativas en materia de protección de datos en los Estados Miembro de la Unión Europea (UE). Cabe señalar que no solo será aplicable a empresas establecidas en la UE, sino también a aquellas empresas que, sin estar establecidas dentro de la UE, traten datos personales de ciudadanos europeos al dirigir sus bienes o servicios a los mismos.
2. **Nuevos derechos de las personas.** Los ciudadanos tendrán más información sobre cómo son tratados sus datos personales. Además de los ya conocidos derechos ARCO (acceso, rectificación, cancelación y oposición), se regula:
 - i. El alcance del **derecho al olvido**, por el que cualquier ciudadano podrá solicitar el borrado definitivo de sus datos personales cuando se dé de baja de un servicio contratado, a excepción de que exista una normativa que lo impida.
 - ii. El **derecho a la portabilidad** de los datos de un usuario, para trasladar sus datos de un proveedor de servicios a otro (i.e., entre distintas redes sociales).
 - iii. **El derecho a recibir información en supuestos “hacking” de datos.**
 - iv. **El consentimiento para el tratamiento de los datos personales**, que deberá ser “claramente inequívoco”. Esta obligación tendrá especial relevancia en casos de datos sensibles (salud) o de menores, debiendo implementar mecanismos fidedignos de obtención y tratamiento de datos.
 - v. **El concepto de “datos sensibles”, se actualiza e incrementa, dando cabida a** otros nuevos como la orientación sexual, datos biométricos, genéticos o creencias filosóficas.

3. **Menor burocracia, menores costes.** El RGPD conllevará una notable reducción de la burocracia (y costes) para las empresas europeas. En particular:

- i. *Desaparece la obligación de inscribir ficheros.*
- ii. Se habilitará una "One stop shop" ("Ventanilla Única"). Mediante la creación de la Autoridad de Control, se podrán efectuar trámites con efectos en toda la UE, ante una única autoridad de protección de datos.

4. **Obligaciones de las empresas.**

- i. Obligación de realizar **Análisis de Riesgos y Evaluaciones de Impacto**. El RGPD pretende garantizar la implementación de medidas de protección de datos desde la etapa inicial de un modelo de negocio ("data protection by design"). No obstante, siempre que se traten datos que puedan suponer un riesgo para los afectados, será obligatorio realizar previamente un análisis de riesgos para determinar el cumplimiento normativo.

ii. Deberán nombrar un **Delegado de Protección de Datos** ("Data Protection Officer /DPO"). Esta figura se concibe como supervisor de la actividad del responsable o del encargado de tratamiento de datos en el cumplimiento de sus respectivas obligaciones. Como novedad más destacable, el DPO deberá desempeñar su actividad con plena independencia (sin recibir instrucciones del responsable o del encargado). Deberá ostentar conocimientos legales y de nuevas tecnologías (no siendo viable, por ende, nombrar al Director de IT de la empresa como se viene haciendo en la mayoría de empresas es nombrado Responsable).

iii. Deberán cumplir escrupulosamente con la normativa aplicable, por cuanto se produce un **incremento ostensible de las sanciones aplicables**. A modo de ejemplo, en supuestos de infracción grave, la sanción podrá consistir en un porcentaje de la facturación global (mundial) de la compañía infractora, con lo que las sanciones podrán ser de millones de euros en el caso de multinacionales que no adecuen correctamente su actividad al nuevo Reglamento.

¿Qué pasos deben seguir las empresas para cumplir con el RGPD?

Durante los dos próximos años, hasta la entrada en vigor del Reglamento, todas las empresas van a tener que seguir cumpliendo con los postulados de la LOPD (o cualquier normativa nacional de un Estado Miembro), y paralelamente, van a tener que revisar sus políticas de IT y de protección de datos, para adecuarlas de una forma paulatina (y por ende, menos traumática), al nuevo RGPD.

Los tiempos en que cumplir el trámite de la LOPD inscribiendo ficheros y elaborando un documento de seguridad, era suficiente, dan paso a una nueva etapa en que la protección de datos deberá formar parte de la propia cultura de la empresa; no en vano, incumplir con

la normativa en materia de protección de datos puede acarrear gravísimas sanciones. Así, en un mundo dirigido inexorablemente a la digitalización, las empresas deberán llevar a cabo una transformación cultural y valorar también los beneficios que aportará el cumplimiento del RGPD a su reputación y, por ende, la confianza de sus clientes.

Dicho proceso será complejo y por ello requerirá necesariamente el asesoramiento de expertos legales. Ponemos a su disposición a nuestro equipo de especialistas del Área de IT&IP de Grant Thornton Barcelona, para resolver cualquier duda que pudiera tener sobre este particular.

