# ADAPTACIÓN DEL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

**RESUMEN**

Desde el 25 de mayo de 2018 es de plena aplicación el Reglamento Europeo de Protección de Datos (GDPR). El GDPR amplía las obligaciones y responsabilidad de las empresas y demás entidades que tratan datos personales, en consonancia con la ampliación de los derechos de privacidad de los ciudadanos. Aplica también a empresas de fuera de la Unión Europea que traten datos personales de ciudadanos de la UE, y prevé importantes sanciones en caso de incumplimiento de los principios básicos de protección de datos (se establecen multas de hasta 10 o 20 millones de euros, o de hasta el 2% o el 4% del volumen de negocio total anual global), subrayando obligaciones de las empresas y entidades como la de prevención y la de responsabilidad proactiva. Asimismo, el pasado 7 de diciembre de 2018 entró en vigor la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). La presente ley cumple una doble finalidad, tal como se deduce de su artículo 1: por un lado, desarrollar el marco regulatorio del GDPR, completando y precisando aquellos aspectos que deben desarrollar los Estados miembros y, por otro lado, la nueva LOPDGDD regula de forma novedosa un catálogo de derechos de la era digital, sistematizado en su Título X. Dichos cuerpos legales no deben ser vistos como una amenaza, sino como una oportunidad, pero es necesario que todos los operadores se asesoren adecuadamente a fin de implementar las medidas necesarias, en sus respectivas organizaciones, para garantizar que están en condiciones de cumplir con el GDPR y la LOPDGDD, y que además, están en disposición de demostrarlo.

El Reglamento General de Protección de Datos (GDPR por sus siglas en inglés), Reglamento UE 2016/679, de 27 de abril de 2016, es de aplicación desde el 25 de mayo de 2018, fecha a partir de la cual es obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro. Por otro lado, desde el pasado 7 de diciembre de 2018, es también de aplicación en España la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

El GDPR se aplica a cualquier empresa establecida en la UE, y también a empresas no establecidas en la UE pero que traten datos personales de ciudadanos de la UE, ya sea para ofrecer bienes y servicios, o controlar su comportamiento dentro de la propia UE (art. 3 GDPR), en cuyo caso tales empresas extracomunitarias deberán designar un representante en la UE que atienda las consultas de las autoridades e interesados (art. 27 GDPR). Todo ello teniendo en cuenta que, en el marco del tráfico jurídico de España, deberá cumplirse además con lo dispuesto en la nueva LOPDGDD.

El GDPR se basa en la prevención y el 'principio de responsabilidad proactiva' de las empresas y demás operadores, lo que implica que cada empresa es responsable de cumplir el GDPR y debe estar en disposición de acreditarlo (arts. 5.2 y 24.1 GDPR). Por ello, es necesario que cada empresa se asesore convenientemente y analice sus actuales procesos de tratamiento de datos

personales, a fin de decidir las medidas necesarias, en función de su propio modelo de negocio, costes de implantación y riesgos existentes para los interesados, en aras de garantizar el cumplimiento del GDPR y la LOPDGDD.

El GDPR establece nuevos derechos para los ciudadanos, adicionales a los ya conocidos derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), como el derecho de supresión o derecho al olvido (art. 17 GDPR), el derecho de limitación (suspensión y/o conservación) del tratamiento (art. 18 GDPR), el derecho a la portabilidad de los datos incluyendo su transmisión entre empresas (art. 20 GDPR) o el derecho a no ser objeto de decisiones en base a procesos puramente automatizados, como la elaboración de perfiles (art. 22 GDPR). La nueva LOPDGDD recoge, concreta y amplía, dentro de los límites establecidos en el GDPR, dicho catálogo de derechos.

La referida ampliación de los derechos de los interesados en el marco del GDPR conlleva, a su vez, un amplio abanico de obligaciones complementarias para las empresas y demás operadores, tales como:

- Las empresas con más de 250 trabajadores deberán llevar un **registro de actividades de tratamiento de datos** (art. 30 GDPR), pero esta obligación no se aplicará a ninguna empresa que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

- La **protección de datos desde el diseño** (por ejemplo, cuando una nueva aplicación para móviles esté en fase de desarrollo) **y por defecto**, garantizando que los datos no sean accesibles a un número indeterminado de personas sin la intervención del interesado (art. 25 GDPR).

- Establecer **mecanismos de notificación de brechas de seguridad** a las autoridades y los interesados (piratería informática, virus, etc.) de los datos que constituyan un riesgo (arts. 33 y 34 GDPR).

- Realizar un **análisis de riesgos** de los tratamientos efectuados.

- Revisar la **adecuación de las medidas de seguridad necesarias según el riesgo**, como puede ser el cifrado de datos o la seudonimización (art. 32.1 GDPR) e implementarlas.

- A partir de los resultados del análisis de riesgos, realizar, cuando corresponda, una **evaluación de impacto relativa a la protección de datos** (art. 35 GDPR).

- En determinados supuestos, designar un Delegado de Protección de Datos que supervise el cumplimiento del GDPR y actúe como punto de contacto de las autoridades competentes (arts. 37-39 GDPR). En este sentido, la nueva LOPDGDD concreta en su artículo 34 los supuestos de designación obligatoria de delegado de protección de datos en más de 16 tipos de entidades, entre las cuales colegios profesionales; centros docentes de cualquier nivel; establecimientos financieros; entidades aseguradoras; entidades que desarrollan actividades de publicidad; prospección comercial o elaboración de perfiles; empresas de seguridad privada o federaciones deportivas que tratan datos de menores de edad.

- También en determinados supuestos, evaluar los riesgos sobre la privacidad antes de efectuar determinados tratamientos, en particular mediante el uso de nuevas tecnologías (art. 35 GDPR).

Además, de estas actuaciones se deberá:

- Adecuar los formularios de recogida de datos con el correspondiente derecho de información.
- Establecer mecanismos y procedimientos para el ejercicio de los de derechos de los interesados.
- Revisión de los encargados del tratamiento de que dispone la empresa para verificar que ofrecen garantías suficientes y adaptación de los contratos suscritos hasta la fecha o redacción de nuevos conforme a las exigencias del GDPR. La nueva LOPDGDD precisa, en su Disposición transitoria quinta, el mantenimiento de la vigencia de los contratos suscritos con el encargado de tratamiento con anterioridad al 25 de mayo de 2018 hasta su fecha de vencimiento acorde con lo dispuesto en el artículo 12 de la anterior LOPD de 1999. Si el contrato es de carácter indefinido, se mantiene su vigencia hasta el 25 de mayo de 2022.
- Redactar o adaptar, según corresponda, la política de privacidad.

Por otro lado, y tal como avanzábamos, la nueva LOPDGDD establece ciertas especialidades y precisiones con respecto al GDPR, entre las que cabe destacar:

- Se reconoce el derecho de las personas a dar instrucciones para el tratamiento de sus datos en el entorno de las Tecnologías de la Información y de la Comunicación tras su muerte. La nueva LOPDGDD realiza una aproximación a la regulación conforme los principios del derecho sucesorio español, posibilitando incluso al "testador digital" a excluir a determinadas personas del acceso a sus datos o de cualquier poder de decisión sobre el tratamiento de los mismos (art. 3 LOPDGDD).
- Se fija la edad mínima, para prestar consentimiento para el tratamiento de datos por menores de edad en 14 años, sin perjuicio de que en edades inferiores pueda ser prestado por los titulares de la patria potestad (art. 7 LOPDGDD).
- El tratamiento de datos especialmente sensibles, relativos a ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico no podrá fundarse en el consentimiento del interesado, si bien si pueden fundarse en las demás causas de legitimación del tratamiento (art. 9 LOPDGDD).
- Se entiende cumplido el requisito de derecho de acceso si se facilita al interesado un sistema de acceso permanente, remoto, directo y seguro a sus datos personales.
- Se define, por otro lado, el concepto de "solicitud repetitiva" del ejercicio de derecho de acceso, cuando se solicita más de una vez en un período de seis meses, salvo causa legítima (art. 13 LOPDGDD).
- Pueden tratarse conforme al principio de interés legítimo los datos de empresarios, profesionales liberales o que desarrollan funciones en personas jurídicas cuando el tratamiento se refiere únicamente a los datos necesarios para su localización profesional y la finalidad es mantener relaciones con la persona jurídica a la que el afectado presta sus servicios (art. 19 LOPDGDD).

- Se considera lícito el tratamiento de datos personales relativos a información crediticia, cuando: 1. Los datos son facilitados por el acreedor; 2. los datos se refieren a deudas ciertas, vencidas, liquidas y exigibles; 3. el acreedor ha informado al afectado; 4. se mantengan tales datos mientras persista incumplimiento con un máximo de 5 años desde el vencimiento (art. 20 LOPDGDD).

- Se establece un plazo máximo de un mes para la conservación de las imágenes captadas mediante videovigilancia, salvo determinadas excepciones. Se considera excluido de la aplicación del RGPD la captación de imágenes por la persona física en el interior de su propio domicilio, pero no las empresas de seguridad privada que realicen tales grabaciones (art. 22 LOPDGDD).

- Se define el concepto de bloqueo de datos como la identificación y reserva de los mismos, adoptando las medidas necesarias para evitar su tratamiento, incluida su visualización (art. 32 LOPDGDD).

Otra de las principales novedades de la nueva LOPDGDD es la regulación en su Título X, de un catálogo de derechos de la era digital, que, si bien requieren de un ulterior desarrollo y concreción normativa, la ley sistematiza del siguiente modo:

- Derecho a la neutralidad en la red.
- Derecho de acceso universal a internet.
- Derecho a la seguridad digital.
- Derecho a la educación digital.
- Protección de los menores en internet.
- Derecho a la rectificación en internet.
- Derecho de actualización de informaciones en medios de comunicación digitales.
- Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.
- Derecho al testamento digital.
- Derecho a la desconexión digital en el ámbito laboral.
- Derecho a la intimidad frente al uso de dispositivos de videovigilancia y grabación de sonidos en el lugar de trabajo.
- Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.
- Derechos digitales en la negociación colectiva.
- Protección de datos de los menores en internet.
- Derecho al olvido en búsquedas por internet.
- Derecho al olvido en servicios de redes sociales y servicios equivalentes.
- Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.

Con el fin de cumplir con el principio de responsabilidad proactiva de los arts. 5.2 y 24.1 del GDPR, es imprescindible documentar todas las actuaciones realizadas para poder acreditar la debida diligencia en el cumplimiento, tanto del propio GDPR como de la nueva LOPDGDD.

Por otro lado, es aconsejable, como sello distintivo en la gestión de la protección de datos, que las empresas y entidades valoren la adhesión a códigos de conducta (art. 40 GDPR) en los que se detallen las prácticas concretas de un sector, incluyendo lo relativo a la protección de datos, por ejemplo en relación con temas tales como la seudonimización o la información proporcionada a los niños y su protección, puesto que ello puede ser tenido en cuenta positivamente en la valoración de posibles sanciones.

Y no podemos dejar de hacer una referencia, precisamente, al sistema de sanciones (art. 83 GDPR) previsto por el GDPR y recogido en la LOPDGDD (art. 70 y siguientes), que establece básicamente dos listados de obligaciones cuyo incumplimiento se sancionaría con multas de hasta 10 o 20 millones de euros, o de hasta el 2% o el 4% del volumen de negocio total anual global de una empresa (optándose por la cifra de mayor cuantía), respectivamente, estando el incumplimiento de los principios básicos

de protección de datos o de las obligaciones que afectan a los derechos de los interesados entre las causas de aplicación de las sanciones más elevadas. La clasificación de la LOPDGDD mantiene el régimen sancionador del GDPR. Sin embargo, clasifica las infracciones en tres grupos: muy graves, graves y leves.

En definitiva, el GDPR pretende generar un espacio europeo de confianza que fomente, precisamente, el desarrollo de la economía en la era digital, dominada por la actividad online y los flujos transfronterizos de datos, a cada segundo, en una escala sin precedentes hasta ahora, y en todos los sectores de actividad.

Por ello, el GDPR –y en consecuencia la nueva LOPDGDD– no deben ser considerados por las empresas como una amenaza, un lastre o una carga burocrática y limitativa de la posibilidad de hacer negocios (como indica el GDPR (Considerando 4), "el derecho a la protección de datos personales no es un derecho absoluto"), sino como un argumento de posicionamiento y como una oportunidad de negocio, perfectamente compatible con el necesario y legítimo desarrollo de la economía.

La prioridad que cada empresa o institución conceda a esta cuestión y la transparencia con que la aborde serán factores competitivos y diferenciadores de cada entidad, lo que explica que el propio GDPR obligue a que en los Estados miembros se promueva la creación —y así se ha recogido en el artículo 38 y 39 de la LOPDGDD– de mecanismos de certificación, sellos y marcas de protección de datos para que las entidades que lo deseen puedan demostrar ante sus interlocutores el cumplimiento de la norma (art. 42.1 GDPR).

## ¿TIENE ALGUNA CONSULTA?

Desde el Área de Protección de datos y Privacidad trabajamos para poder resolver las dudas que pueda plantear esta actualización normativa y su afectación a la actividad de las distintas empresas y organizaciones. Si tiene alguna consulta, no dude en ponerse en contacto con nosotros.

## CONTACTO:

Área de Protección de Datos y Privacidad
**rcd@rcd.legal**
**www.rcd.legal**