

Diciembre 2018

NUEVA LEY DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

RESUMEN

La nueva Ley de Protección de Datos entró en vigor el pasado 7 de diciembre. Esta ley supone la adaptación al ordenamiento jurídico español de la legislación europea en materia de protección de datos. La presente nota informativa desgrana los principales aspectos de esta nueva Ley de gran calado.

La nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante "LOPDGDD"), se compone de noventa y siete artículos, estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

La presente ley cumple una doble finalidad, tal como se deduce de su artículo 1: por un lado, desarrollar el marco regulatorio del Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, (en adelante "RGPD") completando y precisando aquellos aspectos que deben desarrollar los Estados miembros. Por otro lado, la nueva LOPDGDD regula de forma novedosa un catálogo de derechos de la era digital, sistematizado en su Título X.

Datos de las personas fallecidas

Se reconoce el derecho de las personas a realizar instrucciones para el tratamiento de sus datos en el entorno de las Tecnologías de la Información y de la Comunicación tras su muerte. La LOPDGDD realiza una aproximación a la regulación conforme los principios de nuestro derecho sucesorio, 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, si bien los detalles del testamento digital se regulan más detalladamente en el artículo 96 de la LOPDGDD.

Exactitud de los datos

Se recoge el principio general de exactitud de los datos ya reconocido en el RGPD, si bien se establece una limitación de responsabilidad en favor del responsable de tratamiento cuando haya adoptado medidas razonables para la rectificación o supresión de los datos inexactos y estos se hayan obtenido de alguna de las siguientes fuentes: el propio afectado, un intermediario autorizado, otro responsable en virtud del ejercicio del afectado del derecho de portabilidad o hayan sido obtenidos de un registro público.

Consentimiento de menores

Se fija la edad mínima para prestar consentimiento para el tratamiento por menores de edad en 14 años, sin perjuicio de que en edades inferiores pueda ser prestado por los titulares de la patria potestad. Si bien el RGPD contempla una edad mínima de 16 años para que el menor manifieste su consentimiento en el tratamiento de sus datos, se faculta a los estados miembros para fijar una edad inferior, que en ningún caso podrá fijarse por debajo de los 13 años. Como hemos indicado, la nueva LOPDGDD ha fijado este límite en 14 años.

Tratamientos de datos basados en “obligación legal” e “interés público”

Se precisan los conceptos de legitimación de tratamiento basado en “obligación” en base a normas de derecho de la Unión o normas nacionales con rango de ley. Los conceptos de “interés público” o “misión en interés público” deben derivar de competencias otorgadas mediante una norma con rango de ley.

Consentimiento para el tratamiento de datos especialmente sensibles

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 sí pueden fundarse en las demás causas de legitimación del tratamiento.

Tratamiento de datos relativos a infracciones penales

Se contemplan tres supuestos para el tratamiento de datos relativos a condenas e infracciones penales, procedimientos, medidas cautelares y de seguridad. En primer lugar, para finalidad distinta a la investigación, prevención, detección y enjuiciamiento, requieren de habilitación legal mediante norma con rango de ley. En segundo lugar, para el registro completo de datos relativos a infracciones penales se mantiene el marco competencial del sistema de registros administrativos de apoyo a la Administración de Justicia. En tercer lugar, y fuera de estos casos, sólo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

Información por capas y capa básica

Cuando los datos se obtengan del interesado, el deber de información se entiende cumplido cuando se facilita información básica junto a un enlace que contiene la restante información. La información básica debe contener:

1. La identidad del responsable o su representante;
2. La finalidad del tratamiento;
3. La posibilidad de ejercer los derechos de acceso, rectificación, cancelación, oposición, portabilidad y limitación del tratamiento.
4. Si se realizan actividades de tratamiento que implican elaboración de perfiles, debe advertirse de tal circunstancia, así como, de modo expreso, sobre el derecho de oposición en los términos del artículo 22 del RGPD.
5. Si no se obtienen los datos del propio interesado, deben incluirse también:
 - a. Categorías de datos;
 - b. Las fuentes de procedencia de los datos.

Ejercicio de los derechos ARCO por los titulares de la patria potestad

Se prevé la posibilidad de que los titulares de la patria potestad ejerciten los derechos de acceso, rectificación, cancelación, oposición, portabilidad y limitación en nombre y representación de los menores de catorce años.

Derecho de acceso

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.

Tratamiento de datos de profesionales liberales

De conformidad con el Artículo 19, se entiende cumplido el principio de interés legítimo en el tratamiento de 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 en la que el afectado presta sus servicios.

Sistemas de información crediticia

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, liquidadas 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.

Tratamiento de operaciones mercantiles

Se presumen lícitos los tratamientos de datos que puedan derivarse de operaciones de modificación estructural o transmisión de negocios, si estos son necesarios para el buen fin de tales operaciones. Si la operación no concluye, deberán suprimirse los datos.

Videovigilancia

El artículo 22 establece un plazo máximo de un mes para la conservación de las imágenes captadas mediante videovigilancia, salvo determinadas excepciones. Se considera excluida 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.

Sistemas de exclusión publicitaria

Quienes quieran llevar a cabo comunicaciones de mercadotecnia directa, deben realizar previamente consulta a los sistemas de exclusión publicitaria, no pudiendo tratar los datos de afectados que se encuentren en dichas listas, si bien será suficiente la consulta de los sistemas de exclusión publicados por la autoridad de control competente.

Sistemas de información de denuncias internas

Se permite la creación y mantenimiento de canales de información y denuncia interna de entidades de derecho privado para el conocimiento de actos contrarios a la normativa general y sectorial. Deben adoptarse medidas para preservar la identidad y garantizar la confidencialidad de los datos, especialmente de las personas afectadas y las personas denunciantes. Finalmente, se establece un plazo de conservación de los datos máximo de 3 meses, salvo excepciones.

Tratamiento de datos en el ámbito de las funciones de estadística pública

Los organismos competentes para el ejercicio de la función de estadística pública pueden denegar las solicitudes de ejercicio de los derechos del artículo 15 a 22 del RGPD cuando los datos se encuentren amparados por las garantías del secreto estadístico previstas en la ley.

Tratamiento de datos con fines de archivo de interés público

Se considera lícito el tratamiento realizado por las administraciones públicas con fines de archivo de interés público, conforme el RGPD, la nueva LOPDGDD y la Ley 16/1985 de Patrimonio Histórico Español.

Tratamiento de datos relativos a infracciones y sanciones administrativas

Para la licitud de tales tratamientos se requiere:

1. Que los responsables de dichos tratamientos sean competentes para la instrucción o la resolución del expediente sancionador;
2. Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad. En los restantes casos se requiere el consentimiento del interesado o el tratamiento por parte de abogados y procuradores en relación a la información facilitada por sus clientes.

Concepto de bloqueo de datos

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.

Concreción de supuestos de designación obligatoria del Delegado de Protección de Datos (DPO)

El artículo 34 concreta los supuestos de designación obligatoria de DPO en más de 16 tipos de entidades. Entre otras, cabe señalar: 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 traten datos de menores de edad.

Cualificación profesional del DPO

Puede tratarse de una persona física o jurídica, pudiendo ser acreditada mediante mecanismos de certificación. Deberá tenerse en cuenta la obtención de titulación universitaria que acredite conocimientos especializados en derecho.

Régimen sancionador

1. Responsables

- Responsables del tratamiento.
- Encargados del tratamiento.
- Representantes de los responsables y encargados del tratamiento no establecidos en la Unión Europea.
- Entidades de certificación.
- Entidades acreditadas de supervisión de códigos de conducta.

Se excluye del régimen sancionador de la LOPDGDD al DPO.

2. Infracciones

a) Muy graves

Prescriben a los 3 años infracciones como, por ejemplo, no obtener el consentimiento del interesado para el tratamiento, utilizar datos para finalidades no compatibles con las que fueron recogidas sin nuevo consentimiento o base legal.

b) Graves

Prescriben a los 2 años infracciones como, por ejemplo, tratamientos de datos de menores de edad sin su consentimiento o el de los titulares de la patria potestad; no acreditar esfuerzos razonables para demostrar la validez del consentimiento de menores de edad o titulares de la patria potestad; la no designación de representante del responsable o encargado del tratamiento no establecido en la Unión Europea

c) *Leves*

Prescriben al año infracciones como, por ejemplo, la exigencia de pago de canon excesivo cuando se permite el cobro de un canon, para el ejercicio de los derechos del acceso, rectificación, cancelación, oposición, portabilidad y limitación.

3. Sanciones

- Prescriben a los tres años: sanciones con importe superior a 300.000 euros
- Prescriben a los dos años: sanciones con importe entre 40.001 y 300.000 euros
- Prescriben al año: sanciones con importe igual o inferior a 40.000 euros

Derechos en la era digital

- **Derecho a la neutralidad en la red**

Se obliga a los proveedores de servicios de Internet a no discriminar su oferta por motivos técnicos o económicos.

- **Derecho de acceso universal a internet**

Establece el legislador un mandato para reducir la brecha digital a toda la población, ya sea por razones de edad, género, discapacidad o de localización geográfica.

- **Derecho a la seguridad digital**

Se establece un principio general de seguridad y de información para los usuarios en las comunicaciones por internet.

- **Derecho a la educación digital**

Se persigue la inclusión de planes de aprendizaje en el uso de los medios digitales a todos los niveles educativos e, inclusive, el acceso a la función pública.

- **Protección de los menores en internet**

Se establece un mandato para con los titulares de la patria potestad, representantes legales y curadores para la educación de los menores a su cargo en el uso equilibrado y responsable de los dispositivos digitales.

Tal mandato se complementa con la posibilidad de intervención del Ministerio Fiscal en supuestos de utilización o difusión de información personal de menores en redes sociales y servicios de la sociedad de información.

- **Derecho a la rectificación en internet**

Los responsables de redes sociales y servicios equivalentes deben adoptar protocolos adecuados para posibilitar el ejercicio del derecho de rectificación en los términos de la Ley Orgánica 2/1984 reguladora del derecho de rectificación.

- **Derecho de actualización de informaciones en medios de comunicación digitales**

Se reconoce a todas las personas el derecho a solicitar a los medios de comunicación digitales la inclusión de un aviso de actualización en las noticias que conciernan al interesado cuando tal información no refleje la situación actual del mismo y ello pueda causarle un perjuicio.

- **Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral**

Se reconoce por un lado el derecho a la protección de la intimidad de los trabajadores y empleados públicos en el uso de dispositivos digitales puestos a disposición del empleador, pero por otro lado se reconoce la posibilidad del empleador, bajo ciertas condiciones, de acceder al contenido de los mismos, a los efectos del control de cumplimiento de obligaciones

laborales y estatutarias. Deberán tenerse especialmente en cuenta, los requisitos establecidos por el Tribunal Europeo de Derechos Humanos en la sentencia conocida como Barbulescu II.

- **Derecho a la desconexión digital en el ámbito laboral**

Tanto trabajadores como empleados públicos tienen derecho a la desconexión digital, que se define como el derecho de respeto de su periodo de descanso en sus distintas formas. Las distintas modalidades de desconexión digital deberán determinarse por el empleador previa audiencia con los trabajadores.

- **Derecho a la intimidad frente al uso de dispositivos de videovigilancia y grabación de sonidos en el lugar de trabajo**

Si bien se reconoce el derecho de los empleadores a tratar las imágenes obtenidas a través de sistemas de videovigilancia y grabación de sonidos en los términos del Estatuto de los Trabajadores, no se admitirá en ningún caso la instalación de estos sistemas en lugares destinados al descanso o esparcimiento de los trabajadores, como, por ejemplo, vestuarios, aseos o comedores.

- **Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral**

En este caso también se reconoce un derecho del empleador para la utilización de sistemas de control de trabajadores o empleados públicos a través de sistemas de geolocalización en los términos establecidos en el Estatuto de los Trabajadores. En todo caso, el empleador debe informar de forma clara expresa e inequívoca de tales sistemas.

- **Derechos digitales en la negociación colectiva**

Pueden incluirse garantías adicionales de tratamiento de datos en el marco laboral a través de los convenios colectivos.

- **Protección de datos de los menores en internet**

Se garantiza la protección del menor en la divulgación y publicación de sus datos personales a través de los servicios de la sociedad de la información, cuando esta difusión se realiza a través de servicios de la sociedad de la información, se requiere el consentimiento del menor o de sus representantes legales conforme lo dispuesto en la nueva LOPDGDD.

- **Derecho al olvido en búsquedas por internet**

Se obliga a los motores de búsqueda a eliminar las listas de resultados indexados por nombre de personas cuando los enlaces que faciliten fueran inexactos, inadecuados, no pertinentes, no actualizados o excesivos. Ello no impide que sea lícita la conservación de la información publicada en el enlace, ni tampoco impide que puedan encontrarse tales enlaces a través de criterios de búsqueda distintos.

- **Derecho al olvido en servicios de redes sociales y servicios equivalentes**

Se regulan tres supuestos de supresión de datos personales facilitados en redes sociales o servicios análogos. En primer lugar, como regla general, las personas tienen derecho a que sean suprimidos, por simple solicitud, los datos que las mismas publican en redes sociales y servicios análogos. En segundo lugar, cuando tales datos son publicados por terceros, puede solicitarse su supresión, cuando estos datos son inadecuados, no pertinentes, no actualizados, excesivos o por circunstancias personales del afectado que prevalezcan sobre el mantenimiento de los datos. Finalmente, en tercer lugar, se regula un supuesto en el que el afectado puede solicitar la supresión y obtenerla sin dilación ni necesidad de justificar las circunstancias anteriores, en el caso de los datos publicados por él mismo o terceros durante su minoría de edad.

- **Derecho de portabilidad en servicios de redes sociales y servicios equivalentes**

Se extiende el derecho de portabilidad reconocido en el artículo 20 del RGPD a los usuarios de servicios de redes sociales y servicios de la sociedad de la información. Los prestadores pueden conservar copia de la información, sin difundirla por Internet, para el cumplimiento de una obligación legal.

- **Derecho al testamento digital**

Se regula la disponibilidad de los datos en el entorno de las tecnologías de la información y de la comunicación (TIC) de las personas fallecidas, aproximándose a la regulación de nuestro derecho sucesorio.

En concreto, pueden dirigirse directamente a los prestadores de servicio de la sociedad de la información, las personas vinculadas a nivel familiar o de hecho, inclusive herederos, a los efectos de acceder e impartir instrucciones relativas a utilización de los datos, destino y supresión. Esta potestad se extiende al albacea o institución equivalente designada expresamente para tales cometidos. En relación a menores de edad y personas con discapacidad, se ejercen tales potestades mediante los titulares de la patria potestad, representantes legales e incluso por el Ministerio Fiscal de oficio o a instancia de parte.

Vigencia de los contratos del encargado de tratamiento

Se mantiene 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. las entidades que lo deseen puedan demostrar ante sus interlocutores el cumplimiento de la norma (art. 42.1 RGPD).

¿TIENE ALGUNA CONSULTA?

Desde el Área de Protección de Datos y Privacidad trabajamos para poder resolver las dudas que pueda plantear esta nueva ley 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:

Víctor Altimira

Asociado del Área de
Protección de Datos y
Privacidad
valtimira@rcd.legal

Irene López

Asociada del Área de
Protección de Datos y
Privacidad
i.lopez@rcd.legal

www.rcd.legal

Jesús Martrat

Socio del Área de Privacidad y
Farma
jmartrat@rcd.legal