Nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales

12 de diciembre de 2018

El 6 de diciembre de 2018 se publicó en el Boletín Oficial del Estado la nueva **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales** (**"LOPDGDD"**), entrando en vigor al día siguiente de su publicación, el día 7 de diciembre de 2018.

La LOPDGDD tiene como fundamento la adaptación del ordenamiento jurídico español al Reglamento General de Protección (RGPD). Con la entrada en vigor de esta nueva ley, se deroga la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como el Real Decreto-Ley 5/2018, de 27 de julio, aprobado con carácter urgente con el fin de implementar una serie de medidas para adaptar la legislación española al RGPD.

Entre los **aspectos más relevantes que introduce la LOPDGDD**, destacamos los siguientes de manera resumida:

➢ Tratamiento de datos con la finalidad principal de identificar la ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico:

La ley exceptúa el consentimiento como vía de legitimación para el tratamiento de los datos con la finalidad de identificar la anterior información sensible a fin de evitar situaciones discriminatorias.

➢ Deber de información:

Se reconoce el mecanismo de información por capas, facilitando al afectado un contenido mínimo con información básica en una primera capa e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata al resto de información.

➢ Ejercicio de derechos:

Se desarrolla la regulación del RGPD aplicable al ejercicio de derechos de acceso, rectificación, supresión, limitación al tratamiento, portabilidad y oposición. Sin embargo, se establecen determinadas características sobro cómo ejercitar estos derechos:

Derecho de acceso:

- Se entenderá otorgado si el responsable del tratamiento facilitara al interesado un sistema de acceso remoto, directo y seguro a la totalidad de los datos personales.
- Se podrá considerara repetitivo el ejercicio del derecho de acceso en más de una ocasión durante un plazo de seis meses a no ser que exista una causa legítima para ello.
- Se podrán considerar excesivas las solicitudes cuando el interesado elija un medio distinto al ofrecido y que éste suponga un coste desproporcionado, debiendo dicho afectado asumir el coste que su elección comporte.

Derecho de rectificación:

- El afectado deberá indicar en su solicitud a qué datos se refiere así como la corrección necesaria. Estas solicitudes se deberán acompañar de la documentación justificativa de la inexactitud o carácter incompleto de los datos.

Derecho de supresión:

- Cuando la supresión derive del ejercicio del derecho de oposición, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros con fines de marketing directo.

Derecho de limitación del tratamiento:

- Se deberá dejar constancia en los sistemas de información del responsable que el tratamiento está limitado.

➢ Se regulan disposiciones aplicables a tratamientos concretos:

Datos de contacto y datos de empresarios individuales y de profesionales liberales:

Se presume que concurre interés legítimo del responsable del tratamiento conforme a RGPD siempre y cuando:

- El tratamiento se limite a los datos necesarios para su localización profesional;
- la finalidad del tratamiento sea mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios o las relaciones profesionales con empresarios individuales y profesionales liberales.

Sistemas de información crediticia:

Se presume lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito siempre y cuando se cumplan los siguientes requisitos:

- que los datos hayan sido facilitados por el acreedor;
- que se refieran a deudas ciertas, vencidas y exigibles;
- que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquellos en los que participe;
- que los datos solo se mantengan en el sistema mientras persista el incumplimiento, con el límite máximo de 5 años desde la fecha de vencimiento de la obligación.

Operaciones mercantiles (fusiones y adquisiciones):

Se presumen lícitos los tratamientos de datos, incluida su comunicación con carácter previo, que se deriven del desarrollo de cualquier operación de modificación estructural de sociedades o la transmisión de negocio o rama de actividad empresarial, siempre que sean necesarios para el buen fin de la operación y garanticen la continuidad en la prestación de servicios. Si la operación no llega a concluirse, el cesionario deberá suprimir los datos sin la obligación de bloqueo previo.

Videovigilancia:

Se permite el tratamiento de imágenes a través de sistemas de videocámaras o de sistemas de cámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de las instalaciones.

Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad anterior.

Los datos se suprimirán en el plazo de 30 días desde su captación salvo que acrediten la comisión de un delito en cuyo caso deberán ponerse a disposición de las autoridades competentes en un plazo de 72 horas desde que se tuviera conocimiento.

El deber de información se cumple colocando un dispositivo informativo.

Se introducen novedades respecto al tratamiento de datos por el empleador.

Sistemas de exclusión publicitaria:

Se considera lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas. Las entidades responsables de estos sistemas de exclusión deberán comunicar a la autoridad de control competente su creación, su carácter general o sectorial, así como el modo en que los afectados pueden incorporarse. Estos sistemas se harán públicos por las autoridades de control. Asimismo, quienes deseen realizar comunicaciones de marketing directo, deberán consultar previamente los sistemas de exclusión publicitaria que pudieran afectar a su actuación, a no ser que se cuente con el consentimiento para recibir la comunicación.

Denuncias internas:

Es lícita la creación y mantenimiento de sistemas de información para denunciar, incluso anónimamente, la comisión de actos o conductas contrarias a la normativa general o sectorial que fuese aplicable en el ámbito de una entidad privada. Los empleados deberán ser informados de la existencia de estos sistemas de información.

➢ Novedades en el régimen de responsables y encargados del tratamiento.

Supuestos particulares en la adopción de medidas técnicas y organizativas:

Se establecen obligaciones generales del responsable y del encargado para determinar las medidas técnicas y organizativas apropiadas a fin de garantizar y acreditar que el tratamiento es conforme con el RGPD, teniendo en cuenta supuestos particulares como, entre otros: situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

Representantes de los responsables o encargados del tratamiento no establecidos en la Unión Europea:

Se imponen al representante su responsabilidad solidaria junto con el responsable o encargado del tratamiento, cuando traten datos de afectados ubicados en España, sin perjuicio de la responsabilidad que pudiera corresponder al responsable o al encargado del tratamiento y del ejercicio por el representante de la acción de repetición frente a quien proceda.

Bloqueo de los datos:

Se mantiene la obligación de bloquear los datos cuando proceda su rectificación o supresión. El bloqueo consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Transcurrido el plazo, los datos deberán ser destruidos.

Validez de los contratos de encargo del tratamiento:

Los contratos de encargo de tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

➢ Novedades en relación al Delegado de Protección de Datos ("DPO").

Designación de un Delegado de Protección de Datos:

Se estipulan una serie de supuestos en los que las entidades, en todo caso, deberán nombrar un DPO e impone la obligación de notificar el nombramiento a la Agencia Española de Protección de Datos en el plazo máximo de diez días.

Estas entidades son las siguientes:

- Los colegios profesionales y sus consejos generales.
- Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
- Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
- Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
- Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
- Los establecimientos financieros de crédito.
- Las entidades aseguradoras y reaseguradoras.
- Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

- Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
- Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.
- Los centro sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud, que aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.
- Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.
- Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.
- Las empresas de seguridad privada.
- Las federaciones deportivas cuando traten datos de menores de edad.

➢ Garantía de los derechos digitales.

Una de las principales novedades del LOPDGDD ha sido la inclusión de este título X para garantizar los llamados "**derechos digitales**", entre los que se incluyen la **neutralidad de la red**, el **acceso universal a Internet**, la **seguridad digital**, la **educación digital** y la **protección de menores en Internet.**

Asimismo, se introduce el **derecho de rectificación en Internet** que impone a los responsables de redes sociales y servicios equivalentes a adoptar protocolos adecuados para posibilitar el ejercicio de este derecho ante usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet. Además los medios de comunicación digitales deberán publicar un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo.

Se regula el **derecho al olvido en búsquedas de Internet y en redes sociales y servicios equivalentes** cuando los datos personales que conciernan a un individuo sean inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieran devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información, o bien las circunstancias personales del afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se regula también el **derecho a la portabilidad en servicios de redes sociales y servicios equivalentes**: los prestadores de dichos servicios estarán obligados a entregar y transmitir a los usuarios los contenidos que les hubiesen facilitado, así como a otro prestador designado por el usuario, siempre que sea técnicamente posible.

Se introduce el derecho al "**testamento digital**". El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas será posible para las personas vinculadas al fallecido por razones familiares, de hecho o sus herederos, así como la posibilidad de impartir instrucciones sobre su utilización, destino o supresión. La excepción a este derecho será la prohibición expresa de la persona fallecida.

➢ Nuevos derechos digitales en el ámbito laboral.

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

El empleador solo podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores con el fin de controlar el cumplimiento de las obligaciones laborales y de garantizar la integridad de dichos dispositivos. Para ello, se deberán haber especificado de modo preciso los usos autorizados e implementar garantías para preservar la intimidad de los trabajadores como al determinación de los periodos en los que los dispositivos se pueden utilizar para fines privados.

Derecho a la desconexión digital:

Los trabajadores tendrán derecho a la desconexión digital con el fin de garantizar el respeto a su tiempo de descanso, permisos, vacaciones y su intimidad familiar y personal.

La Ley establece que el ejercicio de este derecho se sujetará a lo establecido en la negociación colectiva o lo acordado por la empresa y los representantes de los trabajadores. Las medidas se establecerán en políticas internas así como las acciones de formación y sensibilización del personal.

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

Los empleadores podrán hacer uso de las imágenes de sus trabajadores obtenidas a través de sistemas de videovigilancia para el ejercicio de sus funciones de

control empresarial. Para ello, los trabajadores deberán ser informados de manera previa, expresa, clara y concisa acerca de esta medida.

Utilización de sistemas de geolocalización:

Los empleadores podrán usar sistemas de geolocalización para el ejercicio de sus funciones de control de los trabajadores siempre que estas funciones se ejerzan dentro de su marco legal. Asimismo, los trabajadores deberán haber sido informados de forma expresa, clara e inequívoca acerca de la existencia y características de estos dispositivos.

Derechos digitales en la negociación colectiva:

Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de los derechos digitales en el ámbito laboral.

➢ Novedades relacionadas con el sector público.

Se ha incorporado una disposición adicional primera relativa a las **medidas de seguridad en el sector público**. Así, se establece que el **Esquema Nacional de Seguridad** incluirá las medidas que deban implantarse para garantizar la seguridad de los datos personales, cumpliéndose con ello la obligación de implantar medidas de seguridad adecuadas, en cumplimiento del art 32 de RGPD.

Se modifica la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, por lo que será **obligatoria la publicación del Registro de Actividades de Tratamiento** por parte de las Administraciones Públicas.

➢ Régimen sancionador.

Sujetos responsables:

Están sujetos al régimen sancionador establecido en el RGPD, los responsables y encargados del tratamiento, los representantes de los responsables o encargados de los tratamientos no establecidos en la Unión Europea, las entidades de certificación y las entidades acreditadas de supervisión de los códigos de conducta. El régimen sancionador no es aplicable al DPO.

Infracciones:

La LOPDGDD establece tres niveles de infracciones diferenciándolas en muy graves, leves y leves, así como un listado de supuestos que incurriría en las sanciones del RGPD. Las infracciones prescriben a los tres años las muy graves, dos años las graves y un año las leves.

Prescripción de las sanciones:

Las sanciones prescriben en el plazo de un año aquellas por importe igual o inferior a 40.000 euros; a los dos años aquellas por importe comprendido entre 40.001 y 300.000 euros y a los tres años aquellas por importe superior a 300.000 euros.

ONTIER

Departamento: Tecnología y Propiedad Intelectual
Contacto: Joaquín Muñoz jmunoz@ontier.net