MARIMÓN
ABOGADOS

Cambios relevantes en la LOPD

Diciembre de 2018

Novedades Protección de datos

El pasado jueves 6 de diciembre de 2018, se publicó en el Boletín Oficial del Estado la nueva **ley española de Protección de datos** que entró en vigor al día siguiente, el 7 de diciembre. Esta nueva ley viene a sustituir la anterior LOPD y a desarrollar y concretar determinados aspectos del Reglamento 679/2016 de 27 de Abril que entró en vigor el pasado 25 de mayo. La nueva ley es larga, con alrededor de 100 artículos y multitud de disposiciones adicionales.

La nueva norma no se limita a unas pocas aclaraciones, sino que se trata de algo mucho más profundo que requiere análisis e implementación dentro de cada empresa. Se recogen temas como el listado de infracciones en materia de datos, nuevas normas de aplicación en el ámbito laboral (geolocalización, videovigilancia y otros), obligaciones en materia de bloqueo y conservación de datos, nuevas obligaciones en los canales de denuncias, normas aplicables a determinadas operaciones mercantiles, obligaciones en materia de consentimiento, nuevos derechos digitales y un largo listado de temas relevantes. En esta breve nota vamos a intentar describir algunas de las novedades que incluye la nueva ley:

Principales novedades:

1. Uso de dispositivos digitales por parte de los trabajadores

Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador. Sin perjuicio de ello, el empleador podrá seguir teniendo acceso a los contenidos derivados del uso de medios digitales facilitados a los trabajadores con el único objetivo de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

Las empresas deben establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad. En su elaboración deberán participar los representantes de los trabajadores. El acceso por el empleador al contenido de dispositivos digitales estará sujeto al cumplimiento de determinadas obligaciones.

Los trabajadores deberán ser informados de los criterios utilizados por la empresa.

Se establece un nuevo derecho consistente en la desconexión digital fuera del horario laboral para respetar el tiempo de descanso del empleado, sus permisos y vacaciones, así como su intimidad personal y familiar. El ejercicio de este derecho dependerá de la naturaleza y objeto de la relación laboral.
El empleador, previa audiencia de los representantes de los trabajadores, deberá elaborar una política interna dirigida a éstos, incluidos los que ocupen puestos directivos, en la que se definirán las modalidades de ejercicio del derecho a la desconexión, y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas.

2. Novedades en materia de videovigilancia de los trabajadores

La videovigilancia se podrá utilizar para el control de los trabajadores dentro de los límites previstos en la ley y la jurisprudencia.

Será necesario informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores y, en su caso, a sus representantes, acerca de esta medida.

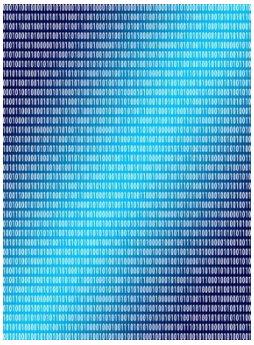
También parece que será posible sancionar al trabajador cuando se haya captado la comisión flagrante de un acto ilícito por los trabajadores siempre que se haya informado a los trabajadores mediante el nuevo cartel informativo de videovigilancia que deberá estar adecuado a la nueva ley.

3. Novedades en materia de geolocalización de empleados

Las empresas podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores, aunque sujeto a varios condicionantes, siempre que se haya informado de forma expresa, clara e inequívoca, a los trabajadores y a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente, deberán informar a los empleados acerca del posible ejercicio de sus derechos.

4. Nuevas infracciones en materia de protección de datos

Una de las novedades del nuevo reglamento europeo es la cuantía de las sanciones en caso de incumplimiento.



Recordemos que las sanciones pueden llegar a 20 millones de Euros o al 4% de la facturación de la empresa o del grupo de empresas en caso de que exista grupo empresarial. Pues bien, la nueva LOPD indica que muchas de las situaciones que se producen frecuentemente en las empresas suponen infracciones graves o muy graves.

Entre otras, son infracciones muy graves:

a) La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos.
b) No informar al afectado acerca del tratamiento de sus datos personales.
c) La vulneración del deber de confidencialidad.
d) No atender el ejercicio de derechos de los usuarios.
e) El incumplimiento de la obligación de bloqueo de los datos.

Entre otras, son infracciones graves:

a) El tratamiento de datos personales de un menor de edad sin recabar su consentimiento o no verificar el consentimiento del menor de edad.
b) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas en cada caso.
c) La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes.
d) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito equivalente.
e) La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable.
f) No disponer del registro de actividades de tratamiento cuando sea necesario.
g) El tratamiento de datos personales sin llevar a cabo una previa valoración de los riesgos.
h) El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.
i) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales cuando sea necesario.
j) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

k) El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible, o no posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

5. Designación de un delegado de protección de datos

La nueva norma obliga a los siguientes tipos de entidades a nombrar un delegado de protección de datos:

a) Los colegios profesionales y sus consejos generales.
b) 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.
c) 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.
d) 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.
f) Los establecimientos financieros de crédito.
g) Las entidades aseguradoras y reaseguradoras.
h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
j) 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.
k) 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.
l) Los centros 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.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.
n) 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.
ñ) Las empresas de seguridad privada.
o) Las federaciones deportivas cuando traten datos de menores de edad.

También establece que las demás empresas podrán nombrar voluntariamente un delegado de protección de datos aunque no sea obligatorio. Además, en el capítulo de infracciones y sanciones se menciona que se considerará el hecho de haber nombrado un delegado de protección de datos a los efectos de graduación de las sanciones, lo que podría hacer recomendable nombrar un DPO a todas las empresas, estuvieran o no obligadas a nombrarlo.

6. Bloqueo de los datos

Se describe la forma en que debe realizarse el bloqueo de los datos cuando haya que suprimirlos o rectificarlos. En particular, la norma establece que cuando sea muy gravoso técnicamente proceder a su bloqueo se podrá realizar un copiado seguro de la información en otro entorno de modo que se permita acreditar la autenticidad de la misma, la fecha del bloqueo y la integridad de los datos.

7. Normas aplicables a los canales de denuncias internas

Se establecen determinadas normas que regulan el tratamiento y conservación de datos en los canales de denuncias cuando se prevé este mecanismo en la implementación de sistemas de *compliance* o cumplimiento normativo.
En principio, la norma establece que los datos en los canales de denuncias no se pueden guardar más tiempo del imprescindible y, de cualquier forma, en ningún caso un plazo superior a 3 meses, aunque podrían guardarse los datos posteriormente a través de otros mecanismos internos o de forma anonimizada.

Por otra parte, las denuncias podrán ser anónimas y será necesario mantener la confidencialidad tanto de la persona denunciante como del contenido de la denuncia.

8. Tratamientos relacionados con la realización de determinadas operaciones mercantiles

Se permite el tratamiento de datos cuando se fusionan o escinden bases de datos como consecuencia de operaciones de reestructuración mercantil o transmisión de negocio, siempre que se continúe el negocio preexistente.

9. Consentimiento

Se confirma, tal como anticipaba el Reglamento europeo, que cuando se solicita el consentimiento para una pluralidad de finalidades se ha de prestar el consentimiento para cada una de ellas. Se establece, a diferencia de lo previsto en el Reglamento, la mayoría de edad a efectos de protección de datos en la edad de 14 años confirmando el criterio que se venía manteniendo en España hasta la fecha.

10. Derechos del interesado

El deber de información del artículo 12 y siguientes del Reglamento, se desarrolla en mayor medida permitiendo diversas posibilidades para ofrecer la información entre la que se encuentra estructurar la información en diferentes capas. En el derecho de acceso se puede solicitar aclaración sobre los datos objeto del ejercicio cuando el volumen de datos del usuario es muy alto, y el solicitante no aclara qué es lo que requiere. Se puede conceder la información solicitada por el usuario por medio de un enlace electrónico a la información.

11. Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales

El tratamiento de este tipo de datos se presume amparado en el interés legítimo siempre que se cumplan varias condiciones (hasta ahora no estaba clara la base del tratamiento).

12. Contratos de encargo del tratamiento

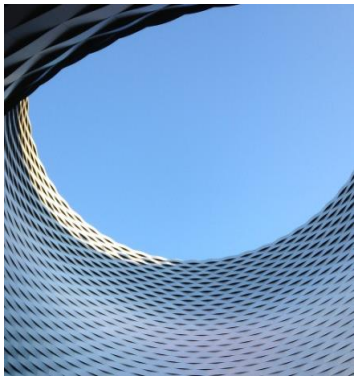
En los contratos de encargo del tratamiento se deberán establecer medidas especiales de prevención desde el punto de vista técnico y organizativo incluyendo la posibilidad de realizar evaluaciones de impacto cuando corresponda. En particular, la ley indica que requerirán un especial análisis y consideración, por su mayor riesgo, entre otras, las siguientes situaciones:

"a) Posibles 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.
b) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679.
c) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos.
d) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.
e) Cuando se produzca un tratamiento masivo de datos.
f) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales".

13. Protección de los menores en Internet

Los padres deberán procurar que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales, y de los servicios de la sociedad de la información. La norma no explica cómo debe llevarse a cabo esta supervisión.

La utilización o difusión de imágenes o información personal de menores en las redes sociales u otros servicios que puedan implicar una intromisión ilegítima en sus derechos fundamentales, requerirá la intervención del Ministerio Fiscal.



14. Derecho a la actualización de informaciones en medios de comunicación digitales

Toda persona tiene derecho a solicitar motivadamente a los medios de comunicación digitales que incluyan un aviso de actualización suficientemente visible, junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.

Marimón Abogados es un despacho fundado en 1931 que ofrece servicios legales en todas las áreas del Derecho y que cuenta con oficinas en Barcelona, Madrid y Sevilla. Nuestro despacho se ha adaptado a los cambios que se han ido produciendo en el mercado mediante la mejora constante de sus servicios y la ampliación de sus ramas de actividad, creando departamentos especializados que cuentan con una dilatada experiencia de acompañamiento a nuestros clientes en su actividad diaria.

— Administrativo y regulatorio
— Concursal
— Fiscal
— Laboral
— Penal
— IP & IT
— Competencia
— Financiero
— Inmobiliario
— Mercantil y societario
— Urbanismo & Medio Ambiente
— Procesal

Italian Desk **French Desk** **German Desk** **Portuguese Desk**

Para cualquier aclaración o comentario sobre el contenido de esta alerta pueden contactar con:

Luis Marimón | Socio del departamento IT/IP
lmarimon@marimon-abogados.com

Elia Pueo | Abogada departamento IT/IP
epueo@marimon-abogados.com

Clara Canut | Abogada departamento IT/IP
ccanut@marimon-abogados.com

Paloma Aparicio | Abogada departamento IT/IP
paparicio@marimon-abogados.com

Juan José Tovar | Abogado departamento laboral
jtovar@marimon-abogados.com