EMLB
ASOCIADOS
GABINETE JURÍDICO-TRIBUTARIO

E-DOSSIER

REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS Y NUEVA LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y GARANTÍAS DIGITALES

¿CUMPLE SU EMPRESA O NEGOCIO CON LAS NOVEDADES SOBRE PROTECCIÓN DE DATOS?

Desde el día 25 de mayo de 2018, viene siendo de aplicación el Reglamento Europeo de Protección de Datos (RGPD), 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.

Además, desde este pasado mes de diciembre ha entrado en vigor en nuestro país la nueva Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales (LOPDGDD), que viene a reemplazar a la ya derogada LOPD 15/1999, para adecuarse al RGPD.

Esto obliga a las organizaciones que tratan datos al deber de valorar la implantación de algunas de las medidas previstas en el RGPD y en la nueva LOPDGDD, en tanto no se puede olvidar que la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española.

El RGPD contiene muchos conceptos, principios y mecanismos similares a los que se articulaban en la también derogada Directiva 95/46/CE, aunque parece ir mucho más lejos en lo referente a la protección de los datos de carácter personal cuando dice en su Considerando número cuatro que: "*El tratamiento de datos personales debe estar concebido para servir a la humanidad.*" En cualquier caso, el RGPD modifica algunos aspectos y contiene nuevas obligaciones que deben ser analizadas y aplicadas por cada organización teniendo en cuenta sus propias circunstancias.

Dos son las principales novedades del mismo:

- **El principio de "accountability" o de responsabilidad proactiva**: por el cual los responsables están obligados a establecer aquellas medidas que consideren apropiadas para garantizar la confidencialidad y protección de los datos personales y, al mismo tiempo, de poder acreditarlo fehacientemente, manteniendo al día la adecuación, actualización y control de cumplimiento necesarios.

- **El enfoque de riesgo**: la aplicación de las medidas previstas por el RGPD debe adaptarse a las características de las organizaciones. De acuerdo con este concepto, las medidas de responsabilidad proactiva deberán de aplicarse en consonancia con el peligro que vaya a comportar el tratamiento para los derechos y libertades de las personas, es decir, a mayor peligro, más medidas protectoras para salvaguardar los datos de carácter personal.

Además de estas innovadoras obligaciones establecidas por el RGPD -que la LOPDyGDD también recoge con el título de "Medidas de responsabilidad activa" en el Capítulo I del Título V, en las que incluye también al encargado del tratamiento-, la entrada en vigor de la Ley Orgánica 3/2018 ha supuesto otra innovación al introducir en su Título X la Garantía de los derechos digitales.

1. CONSENTIMIENTO

El nuevo RGPD mantiene el principio de que todo tratamiento de datos requiere el consentimiento del afectado, salvo contadas excepciones en las que el tratamiento puede estar amparado por una norma legal o para proteger intereses vitales del interesado o intereses legítimos del responsable del tratamiento o de un tercero.

Sin embargo, y a diferencia de la derogada LOPD y de su Reglamento de desarrollo, que admitía formas de consentimiento tácito o por omisión, basadas en la inacción, el nuevo RGPD **exige que el consentimiento se preste mediante un acto afirmativo claro** que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal.

Se contemplan situaciones en las que el consentimiento, además de inequívoco, ha de ser **explícito**:

- Tratamiento de datos sensibles.
- Adopción de decisiones automatizadas.
- Transferencias internacionales.

Especial atención va a merecer el consentimiento de los menores, a los que hacen referencia los artículos 8 RGPD y 7 LOPDGDD, dado que el consentimiento del menor en el RGPD quedaba únicamente circunscrito al tratamiento de los datos personales del menor de edad en la **oferta directa a niños de servicios de la sociedad de la información**, mientras que el ámbito de aplicación en la LOPDGDD será mucho más amplio porque comprende **cualquier tratamiento, tanto automático como manual**, sin limitarse a los servicios de la sociedad de la información.

> ATENCIÓN *A partir de la entrada en vigor del nuevo RGPD, no se podrá seguir obteniendo el consentimiento de los afectados por omisión. Será necesario revisar todos los tratamientos anteriores, para adecuarlos a las previsiones de la nueva normativa.*

2. LA INFORMACIÓN

Asimismo, el deber de informar a los afectados sobre el uso y las finalidades del tratamiento de datos sufre una importante modificación con el nuevo RGPD, pues **se amplía considerablemente la información que se les debe suministrar**, incluyendo aspectos no contemplados hasta la fecha como:

- Base jurídica del tratamiento.
- Intención de realizar transferencias internacionales.
- Datos del Delegado de Protección de Datos (si lo hubiere).
- El plazo o los criterios de conservación de la información.
- La existencia de decisiones automatizadas o elaboración de perfiles.

- El derecho a presentar una reclamación ante las Autoridades de Control.

Además, y en virtud del principio de transparencia, **se exige expresamente que la información se facilite de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo**. En aras a facilitar esta claridad, el nuevo RGPD prevé que la información pueda transmitirse en combinación con **iconos normalizados** que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. En este sentido, la Comisión Europea ya está trabajando en el diseño de estos iconos.

ATENCIÓN *Los procedimientos, modelos o formularios, deberán ser revisados y adaptados al RGPD y a la nueva LOPDGDD, tanto para adaptarlos al nuevo contenido del deber de informar, como para ajustar su forma a los requisitos de precisión y claridad que exige la nueva normativa.*

3. NUEVOS DERECHOS DE LOS AFECTADOS

Los titulares de datos de carácter personal pueden ejercitar ante el responsable del fichero que esté tratando o gestionando sus datos, una serie de derechos.

La LOPD hablaba de 4 derechos básicos (Acceso, Cancelación, Rectificación y Oposición) que se conocían por el anagrama de sus iniciales: DERECHOS ARCO.

El nuevo RGPD incluye nuevos derechos como el derecho a la portabilidad y el derecho al olvido, el derecho a no ser objeto de decisiones individualizadas y el derecho a la limitación del tratamiento.

- **EL DERECHO DE ACCESO**: es un derecho esencial porque el interesado, en tanto que persona física cuyos datos son objeto de tratamiento, debe de poder tener conocimiento de si una organización, sea esta pública o privada, trata sus datos personales como responsable o encargado del tratamiento y, así, poder controlar que se tratan de manera adecuada, sin perjuicio de poder ejercer también otros derechos.

ATENCIÓN *El RGPD reconoce expresamente el derecho de los afectados a obtener gratuitamente una copia de los datos personales objeto de tratamiento.*

En la LOPDGDD se recogen manifestaciones específicas sobre la obligación del responsable de proporcionar información al interesado sobre el ejercicio de sus derechos, entre ellos, el derecho de acceso a la información crediticia del artículo 20.1.c) de la citada Ley Orgánica.

- **EL DERECHO DE RECTIFICACION**: reza el artículo 16 del RGPD: "*El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los*

datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional."

A su vez, el artículo 14 LOPDGDD añade: "*Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.*"

ATENCIÓN *Deberemos de acudir, pues, a los dos textos legales dada su complementariedad para poder ejercer este derecho adecuadamente.*

- **El DERECHO DE OPOSICIÓN**: mediante el ejercicio de este derecho el interesado puede oponerse al tratamiento de sus datos personales en los siguientes supuestos:

  » Cuando no siendo necesario su consentimiento para el tratamiento, exista un motivo legítimo y fundado referente a su concreta situación personal (salvo que una Ley establezca lo contrario).

» Cuando estemos ante tratamientos de datos personales cuya finalidad sea la realización de actividades de publicidad y prospección comercial.

» Cuando el tratamiento tenga como fin la adopción de una decisión referida a su persona, basada únicamente en un tratamiento automatizado de sus datos personales.

- **DERECHO A LA SUPRESIÓN (el derecho al olvido)**: ciertamente imbricado con el principio de limitación del plazo de conservación, en tanto no hay que conservar los datos más tiempo que el estrictamente necesario, los interesados deben de tener derecho a que sus datos se supriman y dejen de tratarse si ya no son necesarios para los fines que fueron recogidos.

  Mención aparte merece este derecho si hablamos de la garantía de los derechos digitales en la nueva LOPDGDD pues ha establecido esta en sus artículos 93 y 94 el "*Derecho al olvido en búsquedas de Internet*" y "*Derecho al olvido en servicios de redes sociales y servicios equivalentes*", respectivamente, y que vienen a representar un derecho de supresión aplicado a tratamientos concretos.

  ATENCIÓN *El derecho a la supresión tiene algunas limitaciones que buscan el equilibrio entre los derechos de supresión y otros intereses relevantes, como la libertad de expresión y el derecho a la información, el interés publico en el ámbito de la salud, la investigación científica o la defensa de reclamaciones.*

- **DERECHO A LA PORTABILIDAD DE LOS DATOS**: podemos identificar este derecho como un instrumento que puede dotar a las personas de un mayor control sobre sus datos personales. Algún autor afirma que el derecho a la portabilidad es un derecho «premium» del derecho de acceso.

  En cualquier caso, deberemos de centrarnos en tres aspectos básicos a la hora de ejercer este derecho:

  » Los datos que pueden ser objeto de ese derecho a la portabilidad.
  » Los requisitos para ejercer el derecho.
  » La forma o manera ce como deberán entregarse los datos.

  Al mismo tiempo, y si bien la LOPDGDD en su artículo 17 solo remite al artículo 20 del RGPD para el ejercicio de este derecho, sí que aporta una regulación adicional que se concreta en el artículo 4.2.c), el cual va a eximir de responsabilidad a aquel responsable del tratamiento que, habiendo adoptado las medidas razonables para suprimir o rectificar los datos inexactos, los someta a tratamiento habiéndolos recibido de otro responsable en virtud del derecho a la portabilidad conforme al artículo 20 RGPD.

- **DERECHO A LA LIMITACIÓN DEL TRATAMIENTO**: este derecho viene a intentar solucionar aquellas situaciones en las que

el interesado se oponía al tratamiento de sus datos o en aquellos casos en que el responsable quería suprimirlos por otra razón y el interesado no quería que se borrasen. Este derecho será susceptible de utilización cuando:

» Se impugne la exactitud de los datos, mientras se verifica dicha exactitud por el responsable.
» El interesado ha ejercitado su derecho de oposición al tratamiento de datos, mientras se verifica si los motivos legítimos del responsable prevalecen sobre el interesado.
» El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.
» El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

- **DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES:** deberíamos de entender este derecho como una especificidad del derecho de oposición, pero en referencia a la analítica del comportamiento para la obtención de perfiles y la singularización de los individuos, lo que comportaría la toma de decisiones basadas en conclusiones extraídas del análisis del comportamiento de los individuos. Es lo que venimos a denominar Big Data, el cual se fundamenta en el avance tecnológico, hecho que va a suponer un reto para el futuro de la privacidad de las personas.

  Este derecho podrá ser ejercido por cualquier interesado, siempre y cuando no concurra alguna de las excepciones que prevé el RGPD.

4. NUEVAS OBLIGACIONES PARA LOS RESPONSABLES

- **ANÁLISIS DE RIESGO**: todos los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo. Así, se deberán de perseguir dos objetivos básicos cuando hagamos una valoración de riesgos:

  » Identificar las medidas de seguridad (tecnológicas, administrativas, orgánicas, etc.) que protejan los datos de carácter personal.
  » Identificar los riesgos asociados a la protección de los derechos y libertades de las personas.

- **REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO**: responsables y encargados deberán mantener un registro de actividades de tratamiento en el que se contenga la información que establece el RGPD y que contenga cuestiones como:

- » Nombre y datos de contacto del responsable o corresponsable y del Delegado de Protección de Datos si existiese.
- » Finalidades del tratamiento.
- » Descripción de categorías de interesados y categorías de datos personales tratados.
- » Transferencias internacionales de datos.
- » Medidas técnicas de seguridad, cuando sea posible.
- » Las categorías de tratamientos efectuados.

ATENCIÓN *Están exentas las organizaciones que empleen a menos de 250 trabajadores, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales. En cualquier caso, este hecho no obsta a hacer un registro de las actividades del tratamiento para certificar la responsabilidad proactiva ante una eventual inspección de la autoridad de control; de hecho, aconsejamos encarecidamente la realización de este registro de las actividades del tratamiento (RAT).*

- **EVALUACIÓN DE IMPACTO**: los responsables de tratamiento deberán realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) con carácter previo (sin que sea un obstáculo realizarlo en tratamientos ya implantados) a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados para evaluar, en especial: el origen, la naturaleza, la particularidad y a gravedad de dicho riesgo. Vale la pena apuntar que no llevar a cabo una EIPD cuando se debería, es una infracción grave.

- **NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD DE LOS DATOS**: cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, en un plazo máximo de 72 horas, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados. En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con una notificación dirigida a estos últimos.

- **DELEGADO DE PROTECCIÓN DE DATOS (DPD)**: según el RGPD este será obligatorio en:

  - » Autoridades y organismos públicos.
  - » Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala.
  - » Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles.

Con la nueva LOPDGDD se amplía esta lista, en tanto la obligación de designar a un DPD -que además ha de cumplir con los requisitos del artículo 35- se debe llevar a cabo en:

» 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 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.
» 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.

ATENCIÓN *Los datos de contacto del DPD deben hacerse públicos por los responsables y encargados del tratamiento porque cuando estos hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame. Asimismo, la designación de un DPD deberá ser comunicado a las autoridades de supervisión competentes.*

5. MEDIDAS DE SEGURIDAD

El Reglamento de Desarrollo de la LOPD determinaba de forma exhaustiva las medidas de seguridad aplicables, según el tipo de datos objeto de tratamiento. En la nueva normativa, las medidas de seguridad no aparecen tan detalladas, sino que **cada organización deberá contar con un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo**.

Además, la tipología de los datos no será la única variable para tomar en consideración a la hora de determinar las medidas técnicas y organizativas aplicables, sino que, por el contrario, el nuevo RGDP tiene en cuenta:

- El coste de la técnica.
- Los costes de aplicación.
- La naturaleza, el alcance, el contexto y los fines del tratamiento.
- Los riesgos para los derechos y libertades.

En cualquier caso, podemos entender que será imprescindible cubrir los tres pilares básicos

para mantener los datos con cierta seguridad ante amenazas, ya sean estas de carácter interno o externo: **Integridad**, **confidencialidad** y **disponibilidad**.

ATENCIÓN *El esquema de medidas de seguridad previsto en el Reglamento de Desarrollo de la LOPD no seguirá siendo válido de forma automática. Es necesario determinar, caso por caso, las medidas aplicables, bajo un enfoque de riesgo, basado en el principio de la seguridad desde el diseño y por defecto.*

6. ENCARGADOS DE TRATAMIENTO

También la figura de los encargados de tratamiento sufre importantes cambios en la nueva regulación. En síntesis, estos cambios se pueden resumir en tres puntos:

1) El RGPD establece **obligaciones expresamente dirigidas a los encargados de tratamiento**, como:

   » Mantener un registro de actividades de tratamiento.
   » Determinar las medidas de seguridad aplicables a los tratamientos que realizan.
   » Designar a un Delegado de Protección de Datos en los casos previstos por el RGPD.

2) Se acentúa el **deber de diligencia en la elección del encargado del tratamiento**, de manera que los responsables habrán de elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas.

3) Se modifica el **contenido mínimo que debe incluir el contrato con el encargado del tratamiento**, incluyendo aspectos como:

   » Objeto, duración, naturaleza y la finalidad del tratamiento.
   » Tipo de datos personales y categorías de interesados.
   » Obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable.
   » Condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones.
   » Asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados.

ATENCIÓN *Se deben revisar todos los contratos de encargo de tratamiento firmados con anterioridad, para verificar si cumplen las nuevas exigencias del RGPD. Aun así, los contratos de encargo de tratamiento de datos personales entre responsables y encargados del tratamiento suscritos antes del 25 de mayo de 2018 mantendrán su vigencia hasta el 25 de mayo de 2022. El contrato deberá de ser por escrito.*

7. TRANSFERENCIAS INTERNACIONALES DE DATOS

El RGPD tiene como objetivo la libre circulación de datos entre los Estados miembros. Sin embargo, esa libre circulación queda supeditada a una serie de normas cuando se habla de Transferencias Internacionales de Datos (TID), es decir, fuera del Espacio Económico Europeo.

Así, la Comisión Europea ha designado una serie de países que, según previa evaluación, gozan de un «**nivel adecuado de protección**» y será posible realizar transferencias internacionales sin ningún tipo de autorización.

En el caso de aquellos países que no gocen de ese adecuado nivel de protección, se podrán hacer transferencias internacionales mediante «**garantías adecuadas**».

Las transferencias internacionales en Grupos Multinacionales podrán ejercerse en base a «**Normas Corporativas Vinculantes**» o «**Binding Corporate Rules**» (**BCRs** por sus siglas en inglés).

En ausencia de cualquiera de las opciones esgrimidas, se podrá seguir llevando a cabo una transferencia internacional de datos si resulta de aplicación alguna de las excepciones que, a tal efecto, plasma el artículo 49 RGPD, aunque se deberán comunicar a la autoridad de control y al interesado de la transferencia, tal y como se refleja en la LOPDGDD.

8. LA GARANTÍA DE LOS DERECHOS DIGITALES

La era informática trae consigo una serie de nuevos derechos susceptibles de proteger y, en este entorno evolutivo, los llamados «**derechos digitales**» abogan por formar parte de ese elenco, en tanto también se les puede relacionar con otros derechos como el de la privacidad, que garantiza el RGPD, y que la LOPDGDD ha querido ampliar y complementar en base al RGPD.

Los derechos a la intimidad, los derechos de uso de dispositivos digitales en el ámbito laboral, así como el derecho al testamento digital, darán mucho que hablar de esta nueva LOPDGDD en los próximos meses.