GTA VILLAMAGNA

ABOGADOS


# ALERTA

## Protección de datos de carácter personal

Marzo 2018

*Modificaciones en el marco regulatorio de las obligaciones exigibles en materia de protección de datos de carácter personal*

## I. INTRODUCCIÓN

En mayo de 2016 entró en vigor el 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 y por el que se deroga la Directiva 95/46/CE (en adelante, el "**RGPD**"), que será **aplicable a partir del 25 de mayo de 2018**.

Nos encontramos, por tanto, en un periodo transitorio, durante el cual **los responsables y encargados del tratamiento de los datos de carácter personal deben ir preparando y adoptando las medidas necesarias para que sus organizaciones estén en condiciones de cumplir con las previsiones del RGPD** en el momento que éstas sean de aplicación y legalmente obligatorias.

En este sentido, ha de tenerse en cuenta que el RGPD es una norma directamente aplicable, que no requiere normas internas de transposición, lo que implica que **los responsables de tratamiento han de asumir que la norma de referencia es el RGPD y no las normas nacionales, como venía sucediendo hasta la actualidad**. No obstante, la nueva ley[1] que sustituirá a la actual Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, **LOPD**), sí podrá incluir algunas precisiones o aspectos de desarrollo en aquellas materias en las que el RGPD lo permite.

En general, el RGPD hace referencia a numerosos conceptos, principios y medidas semejantes a los contenidos en la normativa actual de aplicación, pero, a su vez, **introduce modificaciones en algunos aspectos del régimen actual e incluye nuevas obligaciones que han de ser examinadas e implementadas de manera obligatoria por cada organización según sus particularidades.**

En este contexto, la presente alerta tiene por objeto destacar algunas de las principales novedades, así como las posibles medidas a adoptar por las organizaciones como consecuencia de la aplicación del RGPD, sin pretender ser una exposición exhaustiva de todas las modificaciones introducidas.

En términos generales, para un correcto entendimiento del alcance y significado de las referidas novedades, el RGPD debe ser examinado a la luz del denominado "*principio de responsabilidad proactiva o preventiva*". Este principio exige aplicar la protección de datos desde el punto de vista preventivo y desde el enfoque del riesgo para evitar de manera anticipada la producción de daños a los interesados. Además, obliga a las organizaciones a adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el RGPD establece.

## II. PRINCIPALES NOVEDADES DEL RGPD Y RECOMENDACIONES

A continuación se detallan algunas de las novedades más significativas y recomendaciones para lograr el correcto cumplimiento del RGPD.

[1] Actualmente está tramitándose como "Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal" ante la Comisión de Justicia a la espera de la aprobación del texto definitivo por las Cortes.

## I. El consentimiento del interesado

El RGPD establece como novedad que el consentimiento debe ser inequívoco, por lo que ya no será posible obtenerlo de manera tácita o por omisión, ni tampoco a través de cláusulas de obtención del consentimiento demasiado extensas o incomprensibles. Así, las organizaciones deberán utilizar un lenguaje mucho más riguroso, lo cual implicará que el consentimiento:

- se haya prestado mediante "*una manifestación del interesado o mediante una clara acción afirmativa*";
- sea distinguible mediante la utilización de términos claros y simples; y
- sea revocable en cualquier momento.

Con carácter adicional, se contemplan situaciones en las que, aparte de inequívoco, el consentimiento ha de ser explícito cuando: (i) exista tratamiento de datos sensibles; (ii) se adopten decisiones automatizadas; o (iii) haya transferencias internacionales de datos.

Finalmente, se prohíbe que la prestación del servicio esté condicionada a la obtención de un consentimiento que no sea necesario para ejercer o prestar dicho servicio.

Por tanto, para cumplir con estos nuevos requisitos, resulta recomendable:

- ✓ Revisar y analizar los tratamientos que se llevan a cabo.
- ✓ En ningún caso obtener el consentimiento por omisión o tácitamente.
- ✓ Analizar y, en su caso, elaborar nuevos formularios por los que se recaban los consentimientos de los interesados[2].
- ✓ Implementar medidas técnicas que permitan acreditar que el consentimiento del interesado ha sido válidamente obtenido.

## II. La transparencia e información al interesado

La LOPD exige que la información relativa a la recogida y tratamiento de los datos se proporcione de manera expresa, precisa e inequívoca. Sin embargo, ahora el RGPD obliga a que, al amparo del principio de transparencia, la información se facilite de manera concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

Por tanto, se deberán evitar las cláusulas informativas especialmente farragosas, explicando el contenido al que se refieren de manera clara y accesible para los interesados. Además, esta información deberá constar por escrito.

A este respecto, el RGPD establece una lista exhaustiva de la información que debe proporcionarse a los interesados y que añade, con respecto a la información requerida por la LOPD, la siguiente información:

- La base jurídica del tratamiento;
- Si existe o no intención de realizar

[2] En relación con este aspecto la Agencia Española de Protección de Datos ha señalado que no será posible convalidar aquellos consentimientos antiguos que no cumplan con la nueva regulación. Por tanto si, a la luz del nuevo RGPD, dicho consentimiento no es válido será necesario obtener de nuevo el consentimiento válido de todos los sujetos afectados.

transferencias de datos internacionales;

- Los datos de contacto del Delegado de Protección de Datos (si éste existe); y
- La existencia de decisiones automatizas, incluida la elaboración de perfiles.

Con el fin de que las empresas se adapten a estas obligaciones, la Agencia Española de Protección de Datos (en adelante, "**AEPD**") ha elaborado una "*Guía para el cumplimiento del deber de informar*", en la que se sugiere la implementación de un modelo "por capas". Así, en la primera capa se ofrecerá al interesado cierta información de carácter básico sobre los aspectos más relevantes (responsable del tratamiento, finalidad, destinarios, derechos y legitimación), que irá seguida de una segunda capa donde se detallará toda aquella información que con carácter específico exige el RGPD.

Para cumplir con estos nuevos requisitos se recomienda:

- ✓ Revisar, y en su caso modificar, el contenido las políticas de privacidad para permitir una compresión eficaz y rápida de las mismas.
- ✓ Añadir en el contenido de las cláusulas informativas sobre protección de datos de carácter personal la información requerida por el RGPD.

## III. Los nuevos derechos de los interesados

El RGPD añade, a los tradicionales derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), los siguientes derechos para mejorar la capacidad de decisión y control de los interesados sobre sus propios datos personales:

- Derecho de supresión (el "Derecho al olvido");
- Derecho a la limitación del tratamiento;
- Derecho a la portabilidad de los datos; y
- Derecho a no ser objeto de decisiones individualizadas.

En este ámbito, será también necesario que el responsable proporcione medios para que las solicitudes de ejercicio de estos derechos se formulen telemáticamente, debiendo informar al interesado sobre las actuaciones derivadas de su petición en el plazo de un mes[3]. Así, en caso de que el responsable decida no atender a una solicitud, el RGPD exige que se motive la negativa informando al interesando en el plazo de un mes a contar desde la presentación de la solicitud.

Por ello, es aconsejable para las organizaciones que actúan como responsables del tratamiento, implementar en sus procedimientos de información los nuevos derechos que asisten a los interesados.

## IV. Las nuevas categorías de "datos especiales"

Diferenciándose de la anterior regulación, el RGPD elimina la denominación de "datos sensibles" y califica a este conjunto bajo el término de "datos especiales". Además prevé tres nuevas categorías de datos

[3] Este plazo podrá ampliarse a dos meses más cuando se trate de solicitudes especialmente complejas.

especiales:

- los datos genéticos;
- los datos biométricos (por ejemplo, la huella dactilar); y
- Las creencias filosóficas.

Así, para cumplir con estas novedades se recomienda:

- ✓ Analizar la naturaleza de todos los datos personales que están siendo tratados por la organización, con especial atención a aquellos datos que queden incluidos ahora bajo estas categorías.
- ✓ En relación con aquellos datos que sean de carácter "especial" se deberá: (i) verificar las medidas técnicas y de seguridad que están siendo implementadas para el tratamiento de este tipo de datos; (ii) examinar los formularios de consentimiento relativos a la obtención de estas categorías de datos; y (iii) comprobar si existe algún prestador de servicio con acceso a este tipo de datos.

## V. Obligaciones en relación con el encargado del tratamiento

Otro de los cambios relevantes introducidos por el RGPD es el refuerzo de algunas medidas relativas a las obligaciones de los encargados del tratamiento, como son: (i) la llevanza de un registro de actividades del tratamiento; (ii) la determinación de las medidas de seguridad aplicables a sus tratamientos; y (iii) la designación de un Delegado de Protección de Datos (cuando proceda).

Con carácter adicional, el RGPD impone a los responsables del tratamiento un nivel de diligencia en la elección del encargado del tratamiento. En efecto, se requiere que el responsable únicamente se relacione con encargados del tratamiento que ofrezcan garantías suficientes, en términos de aplicación de medidas técnicas y organizativas, para demostrar de manera anticipada la capacidad de cumplir con los requisitos del RGPD[4].

En línea con lo establecido en la LOPD, el RGPD también obliga a los responsables a suscribir un contrato (por escrito) con cada uno de los encargados del tratamiento. No obstante, el RGPD ha especificado un contenido mínimo que debe incluirse en todos los contratos que se suscriban con encargados. Así, como mínimo, debe establecerse el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y las obligaciones y derechos del responsable del tratamiento.

Así, para facilitar la elaboración de los contratos con encargados del tratamiento, la AEPD ha publicado un documento denominado "*Directrices para la elaboración de contratos entre responsables y encargados del tratamiento*", donde se identifican los puntos clave a tener en cuenta en el momento de establecer la relación entre el responsable y el encargado del tratamiento.

En este contexto, se recomienda:

- ✓ Revisar el contenido de los acuerdos existentes con todos los proveedores de la organización, ya que, en la medida que tengan acceso a datos o,

[4] Para demostrar que los encargados de tratamiento ofrecen garantías suficientes se prevé su adhesión a códigos de conducta u obtener la oportuna certificación en el marco establecido por el RGPD.

si prestan servicios a terceros, deberán ser actualizados.

- ✓ Adaptar el contenido de los citados contratos con el fin de que cumplan con los requisitos exigidos por el RGPD.

## VI. Las medidas de responsabilidad activa

Como se ha señalado, uno de los objetivos del RGPD es establecer diversas medidas que impidan, de manera previa, la eventual producción de daños a los interesados, obligando a las organizaciones a adoptar medidas que aseguren anticipadamente de manera razonable que están en condiciones de cumplir con el RGPD.

Las principales medidas son las que se describen en los siguientes apartados:

### a) El registro de actividades de tratamiento

Ya se ha apuntado la obligación del encargado del tratamiento de implementar, en su caso, un registro de las actividades de tratamiento que realiza por cuenta del responsable. Esta obligación también es exigible al responsable del tratamiento.

El RGPD exime de esta exigencia a aquellas empresas u organizaciones que empleen a menos de 250 personas, a menos que: (i) el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados; (ii) no sea ocasional; o (iii) incluya categorías especiales de datos personales, lo que les obligará a llevar el correspondiente registro.

Así, a partir de mayo de 2018 ya no será necesario declarar nuevos ficheros ante la AEPD, ya que este requisito se sustituye por la obligación interna de la organización de establecer el correspondiente registro de actividades de tratamiento.

El RGPD establece la estructura y el contenido que debe incluir el registro para cumplir con la normativa aplicable: (i) el nombre y los datos del responsable; (ii) los fines del tratamiento; (iii) descripción de las categorías de interesados y de datos personales; (iv) categorías de destinatarios de los datos personales; (v) en su caso, las transferencias internacionales de datos; (vi) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos; (vii) cuando sea posible, la descripción general de las medidas técnicas y organizativas de seguridad.

### b) El análisis de riesgos

El RGPD ha aprovechado las ventajas que ofrece la gestión de riesgos, poniendo énfasis en la reflexión sobre las implicaciones que los tratamientos de datos pueden tener en los interesados. Así, el análisis de riesgos trata de prever hasta qué punto un tratamiento (por sus características, tipo de datos o tipo de operaciones) puede repercutir negativamente en los derechos y libertades de los interesados.

Por tanto, el análisis del riesgo se concibe como un estudio de las actividades de tratamiento que se llevan a cabo por la organización con el objetivo de determinar el potencial riesgo al que estén expuestas.

A partir de este análisis y, de ser el caso, con la documentación que conste en el registro de actividades de tratamiento, se podrá determinar si el tratamiento supone o no un alto riesgo para los derechos y libertades de las personas físicas.

Gracias a los resultados de este análisis, el responsable y el encargado del tratamiento aplicarán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo asociado a las actividades de tratamiento.

Para facilitar las actuaciones de las organizaciones en este contexto, la AEPD ha publicado la "*Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*", con el fin de ofrecer directrices y orientaciones para establecer una hoja de ruta que permita contemplar la privacidad mediante un enfoque de análisis de riesgos facilitando el cumplimiento del RGPD.

**c) Las evaluaciones de impacto**

La aplicación del RGPD no implica la necesaria obligación de llevar a cabo una evaluación de impacto. En efecto, el RGPD prevé que la evaluación de impacto se realice "*antes del tratamiento*"[5] y, únicamente, en los casos en los que del análisis previo se desprenda que es probable que exista un alto riesgo para los derechos y libertades de los afectados.

En este sentido, se ha establecido un listado no exhaustivo de tratamientos en los que se considera que existe un alto riesgo en el tratamiento y que, por ende, requerirán de una evaluación de impacto:

- La elaboración de perfiles;
- Los tratamientos a gran escala[6] de datos sensibles; y
- La observación a gran escala de una zona de acceso público.

Esta herramienta es de carácter preventivo y permite, al responsable del tratamiento[7] identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento. A tal efecto, la evaluación de impacto permite establecer el nivel de riesgo que existe con respecto al tratamiento en aras de determinar las medidas de control más adecuadas que sirvan para minimizar el riesgo hasta un nivel aceptable.

A los efectos de realizar una evaluación de impacto se ha de disponer de una metodología que recoja los elementos establecidos por el RGPD, que son, como mínimo:

- la descripción sistemática de la actividad de tratamiento prevista;
- la evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad;
- la evaluación de los riesgos; y
- las medidas previstas para mitigar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que avalen un nivel adecuado de

[5] Ello da lugar a que la evaluación de impacto no deba, por lo general, realizarse sobre aquellas operaciones de tratamiento que ya estén en curso a 25 de mayo de 2018. No obstante, la excepción a esta regla está representada por aquellos casos en los que se produzcan cambios en los riesgos que el tratamiento implica.

[6] Para valorar si existe un tratamiento a gran escala deberá tenerse en cuenta: (i) el número de interesados afectados; (ii) el volumen y la variedad de datos; (iii) la duración de la actividad de tratamiento; y (iv) la extensión geográfica del tratamiento.

[7] La obligación de llevar a cabo una evaluación de impacto corresponde al responsable del tratamiento, contando con la colaboración y ayuda del encargado del tratamiento, y en su caso, con el Delegado de Protección de Datos.

protección.

Además, debe tenerse en cuenta que en el RGPD se prevé que la evaluación de impacto es un proceso que no se agota cuando se finaliza, sino que el tratamiento debe estar sometido a una revisión continua para comprobar si sigue siendo conforme a la evaluación realizada en su día.

A tal efecto, la AEPD ha elaborado la "*Guía para la evaluación de impacto en la protección de los datos personales*", en la que se incluyen directrices y orientaciones sobre cómo definir e implementar una metodología para realizar una evaluación de impacto.

**d) La comunicación de los fallos de seguridad**

El régimen normativo aplicable con anterioridad al RGPD preveía que únicamente determinadas empresas tenían la obligación de comunicar los fallos de seguridad a la autoridad de protección de datos. Sin embargo, el RGDP extiende la obligación de notificar las violaciones de seguridad a todas las organizaciones, a ser posible, en un plazo máximo de 72 horas[8]. No obstante, la notificación a la autoridad no será necesaria cuando exista una baja probabilidad de que la violación suponga un riesgo para los derechos o libertades de los interesados.

Cuando, además, el fallo de seguridad implique un alto riesgo para los derechos o libertades de los interesados, la comunicación a la autoridad deberá incluir una notificación dirigida a los ciudadanos afectados por éste.

**e) La figura del Delegado de Protección de Datos**

El RGPD prevé, con carácter novedoso y como uno de los ejes principales del principio de responsabilidad activa, el establecimiento de la figura del Delegado de Protección de Datos (en adelante, "**DPD**"), cuya función consiste en ser garante del cumplimiento de la normativa de protección de datos en las organizaciones.

A tal efecto, la obligación de nombrar a un DPD se limita a los siguientes supuestos:

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

Con el fin de acotar y definir la terminología empleada en los tres supuestos anteriores, la AEPD, en la 9ª Sesión Anual Abierta (celebrada en mayo de 2017), se pronunció sobre qué entidades deben contar con un DPD, por entender que cumplen con los criterios anteriores. Estas serían, con carácter no taxativo, las siguientes:

- Entidades aseguradoras y reaseguradoras;
- Distribuidores y comercializadores de

[8] Cuando la notificación no pueda realizarse en este plazo, la notificación del fallo de seguridad deberá ir acompañada de una explicación de los motivos causantes del retraso.

energía eléctrica o gas natural;

- Entidades responsables de sistemas de información crediticia;
- Entidades que desarrollen actividades de publicidad que impliquen análisis de preferencias o elaboración de perfiles;
- Centros sanitarios;
- Centros docentes que ofrezcan enseñanzas regladas y las Universidades;
- Colegios profesionales;
- Entidades dedicadas al juego *on line*.

Además de los supuestos obligatorios para la designación de un DPD, los responsables y encargados del tratamiento podrán, de manera voluntaria, designar a un DPD con el objetivo de potenciar el cumplimiento preventivo de sus obligaciones en materia de protección de datos a través de esta figura.

El RGPD permite que el DPD sea un miembro del personal de la organización o que se contrate uno externo en el marco de un contrato de servicios[9], pero siempre deberá ser nombrado atendiendo a sus cualificaciones profesionales, a su conocimiento de la legislación y la práctica de protección de datos, además de cumplir con los siguientes requisitos: (i) total autonomía en el ejercicio de sus funciones; (ii) relación con el nivel superior de la dirección de la organización; y (iii) que se le faciliten todos los recursos necesarios para desarrollar su actividad.

**f) La aplicación de las medidas de seguridad**

En el RGPD se prevé que las medidas de seguridad a aplicar por las organizaciones sean específicas y adecuadas al riesgo en el tratamiento que lleve a cabo la organización.

Así, el RGPD impone la obligación de adoptar las medidas técnicas y organizativas adecuadas a la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como a los riesgos de diversa índole y a la gravedad para los derechos de las personas, debiendo, como mínimo, implantarse las siguientes:

- la seudonimización y el cifrado de datos personales[10];
- la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes en los sistemas y servicios de tratamiento;
- la capacidad de restaurar la disponibilidad y el acceso a los datos de forma rápida en caso de incidente; y
- un proceso de verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Por tanto, con el objetivo de cumplir con las medidas de responsabilidad activa impuestas por el RGPD, se recomienda:

[9] En la medida en que el RGPD prevé que el DPD deberá tener acceso a los datos que se traten, cuando se opte por esta posibilidad, se deberá suscribir también el correspondiente contrato de encargado del tratamiento con el DPD.

[10] La seudonimización se refiere a la sustitución de un atributo por otro en un registro. El cifrado es aplicar un conjunto de técnicas que aseguren que un mensaje solo es comprensible por el destinatario del mismo.

- ✓ Analizar las circunstancias de la organización para determinar si existe la obligación de implantar el registro de actividades de tratamiento.
- ✓ Llevar a cabo un análisis de riesgos del tratamiento que especifique el potencial riesgo al que están expuestos los tratamientos que se realizan por la organización.
- ✓ Implantar un sistema de respuesta y notificación de fallos de seguridad que cumpla con los requisitos establecidos por el RGPD.
- ✓ Examinar las circunstancias y el tratamiento realizado por la organización en aras de determinar si existe la obligación de nombrar a un DPD.
- ✓ Adoptar las medidas de seguridad mínimas establecidas por el RGPD y valorar la implantación de aquellas que sean adecuadas a la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como a los riesgos y gravedad para los derechos de las personas.

# CONTACTOS

Para más información pueden ponerse en contacto con:

**Ernesto García-Trevijano Garnica**

(+34) 91 781 35 28

ernestogtrevijano@gtavillamagna.com

**Marta Plaza González**

(+34) 91 781 35 28

martaplaza@gtavillamagna.com

GTA VILLAMAGNA

ABOGADOS

Síguenos en:

La presente Alerta de Protección de Datos se ha cerrado a fecha 8 de marzo de 2018

Esta Alerta contiene, exclusivamente, información de carácter general y no constituye, ni pretende constituir, asesoramiento jurídico alguno sobre las materias contenidas en ella. Cualquier decisión o actuación basada en su contenido deberá ser objeto del adecuado asesoramiento profesional.



GTA Villamagna Abogados, S.L.P.

GTA Villamagna, Marqués de Villamagna,

3.-6º, 28001 Madrid (España)