AUTO CON TROL
Asociación para la Autorregulación de la Comunicación Comercial

GUÍA DE ADAPTACIÓN AL

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

PARA EL SECTOR PUBLICITARIO

ÍNDICE

01 NUEVO ENFOQUE: LA RESPONSABILIDAD PROACTIVA Pág. 4

02 EL CONSENTIMIENTO Y EL INTERÉS LEGÍTIMO Pág. 5

03 INFORMACIÓN PARA LOS USUARIOS Pág. 8

04 REALIZAR UNA EVALUACIÓN DE IMPACTO Pág. 10

05 OTRAS CUESTIONES A TENER EN CUENTA Pág. 12

06 PRÓXIMOS PASOS Pág. 16

A partir del 25 de mayo de 2018, el régimen de protección de datos de la Unión Europea sufrirá el mayor cambio de las dos últimas décadas. En esta fecha, el Reglamento General de Protección de Datos[1] (RGPD) comenzará a aplicarse en todos los Estados miembros.

Con el RGPD se pretende armonizar la aplicación del marco de protección de datos entre los distintos Estados, buscando uniformidad y coherencia ante la diversidad de normas nacionales y su diferente aplicación por parte de las autoridades de protección de datos.

Además, como novedad respecto del marco anterior, **el RGPD aplica, no solo las empresas establecidas en la Unión Europea, sino también a aquellas empresas de terceros países que ofrezcan productos o servicios a ciudadanos en la Unión o monitoricen su comportamiento en la Unión.**

Esta guía pretende sensibilizar a las empresas sobre los principales cambios y novedades que introduce la nueva norma europea, especialmente en la medida que afecta a su actividad publicitaria.

ASPECTOS PRINCIPALES PARA ADAPTARSE AL RGPD EN EL ÁMBITO PUBLICITARIO

[1] 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 (Reglamento general de protección de datos).

01

NUEVO ENFOQUE: LA RESPONSABILIDAD PROACTIVA

El RGPD apuesta por un esquema que descansa sobre la **responsabilidad proactiva** de las empresas, más conocida por el término anglosajón "*accountability*".

Esto se traduce en que la empresa deberá:

01. Realizar un constante esfuerzo, no solo por cumplir la normativa de protección de datos, sino por ser capaz de demostrarlo.
    - Esto exigirá a la empresa que documente todas las medidas y decisiones que se adopten en relación con esta materia.

02. Sujetar su actuación al principio de **protección de datos desde el diseño.**
    - Lo que obliga a la empresa a pensar en términos de protección de datos desde la fase inicial del tratamiento, implementando medidas técnicas y organizativas para cumplir de forma efectiva el RGPD.

03. Cumplir el principio de **protección de datos por defecto.**
    - Debiendo aplicar las medidas apropiadas para garantizar que, por defecto, solo se tratan los datos necesarios para los fines específicos que se persiguen con el tratamiento.

Las compañías deberán tener en cuenta el RGPD desde el momento en que se decida llevar a cabo cualquier acción publicitaria en la que se obtengan o utilicen datos personales

Por lo tanto, es importante que la empresa tenga en cuenta el RGPD desde el momento en que decida llevar a cabo cualquier acción publicitaria en la que se obtengan o utilicen datos personales, desde la fase de concepción y planteamiento, adoptando las medidas necesarias para cumplir el RGPD.

02

EL CONSENTIMIENTO Y EL INTERÉS LEGÍTIMO

A partir de la entrada en vigor del RGPD habrá distintas bases jurídicas que legitimarán los tratamientos de datos (entre otras, el consentimiento y el interés legítimo). Las empresas deberán determinar, a la vista de las circunstancias del concreto tratamiento, cuál es la base jurídica más apropiada para legitimarlo.

EL CONSENTIMIENTO

En España, la base jurídica que tradicionalmente ha justificado el tratamiento con fines publicitarios ha sido el consentimiento, que en ocasiones incluso podía ser tácito, es decir, obtenerse por la inacción del interesado.

Sin embargo, **el RGPD excluye el consentimiento tácito**, ya que entiende el consentimiento como una *"manifestación de voluntad libre, específica, informada e inequívoca"*, que debe darse *"mediante una declaración o una clara acción afirmativa"*. Por lo tanto, *"el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento"*.

El silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento

Esto es especialmente importante porque los tratamientos que se basen en el consentimiento tácito dejarán de ser válidos a partir del 25 de mayo de 2018, salvo que se obtenga un nuevo consentimiento conforme al RGPD o concurra otra base jurídica que los legitime.

Cuando los datos pretendan utilizarse para distintas finalidades, **es importante que la empresa obtenga el consentimiento para cada una de ellas, ya que en otro**

caso se presumirá que ese consentimiento no es libre. Por lo tanto, si la empresa recoge el consentimiento para finalidades de tratamiento distintas, con carácter general deberá obtener consentimientos separados.

Si la empresa recoge el consentimiento para finalidades de tratamientos distintas, con carácter general deberá obtener consentimientos separados

Además, condicionar un contrato a que el interesado consienta un tratamiento de datos que no es necesario para el cumplimiento de dicho contrato (por ejemplo, condicionar una prestación de servicios a que se acepte el envío de publicidad) también dará lugar a que se presuma que el consentimiento no es libre.

El RGPD exige en ocasiones un **consentimiento explícito**, que es aquel que se presta de forma clara y determinada, sin que pueda simplemente desprenderse de una acción del interesado. Así, por ejemplo, seguir navegando en una página web para aceptar el uso de cookies cumple las condiciones del consentimiento "estándar" del RGPD, pero no las condiciones del consentimiento explícito. Para la obtención del consentimiento explícito será necesario incluir, por ejemplo, una casilla sin premarcar en la que se indique lo que está consintiendo el usuario (el llamado "*opt-in*").

La empresa deberá obtener un consentimiento explícito, entre otros casos, **cuando trate categorías especiales de datos** (comúnmente llamados "datos sensibles")[2] y también cuando pretenda adoptar una decisión basada únicamente en un tratamiento automatizado, incluida la **elaboración de perfiles**, que produzca efectos jurídicos en el interesado o le afecte significativamente de modo similar (por ejemplo, el uso de técnicas de *scoring* para determinar qué tipo de oferta sobre un producto financiero se puede hacer a una persona).

El RGPD permite a los Estados miembros fijar la edad mínima para prestar el consentimiento sin consentimiento o autorización de los padres o tutores en una edad comprendida entre los 13 y los 16 años. En caso español, el

[2] Se consideran categorías especiales aquellos datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical; y también los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona y los datos relativos a la salud o a la vida sexual u orientación sexual.

Proyecto LOPD[3] fija la edad en 13 años. Si el consentimiento o autorización de los padres o tutores es necesario, la empresa deberá hacer esfuerzos razonables para comprobar que se ha dado ese consentimiento o autorización, teniendo en cuenta la tecnología disponible.

EL INTERÉS LEGÍTIMO

El tratamiento de datos personales con fines publicitarios también podrá basarse en el **interés legítimo** de la empresa, al menos cuando se trate de comunicaciones comerciales no electrónicas, siempre que este interés prevalezca sobre los intereses o los derechos y libertades fundamentales de los interesados.

La Agencia Española de Protección de Datos ha entendido que deben concurrir estos requisitos para que exista ese interés legítimo prevalente para el envío de publicidad:

- cumplir el deber de información (ver apartado 3);
- permitir la oposición a estos envíos;
- el destinatario tiene que ser un cliente activo de la entidad; y
- los productos o servicios ofertados tienen que ser propios de la entidad y similares a los contratados inicialmente, a la vista de las expectativas razonables del cliente[4].

Además, si se quieren enviar **comunicaciones comerciales por vía electrónica, la empresa deberá haber obtenido el consentimiento expreso de sus destinatarios,** salvo cuando exista una relación contractual previa y las comunicaciones se refieran a productos o servicios propios similares a los inicialmente contratados, en cuyo caso el envío de comunicaciones comerciales será válido siempre que se permita la oposición tanto en el momento de recogida de los datos, como en cada comunicación enviada (el llamado "*opt-out*").

No obstante, debe tenerse presente que este régimen previsto para los medios digitales se verá desplazado por el **Reglamento de ePrivacy,** cuya propuesta está siendo aún objeto de negociación en el seno de las instituciones europeas y podría introducir cambios a este respecto.

[3] Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal publicado en el Boletín Oficial de las Cortes Generales con fecha de 24 de noviembre de 2017.

[4] Informe 0195/2017 del Gabinete Jurídico.

03

INFORMACIÓN PARA LOS USUARIOS

La AEPD, en su Guía para el cumplimiento del deber de informar, recomienda facilitar la **información por capas**

Las empresas deberán ampliar la cantidad de información proporcionan a los interesados previamente al tratamiento de los datos. Esta información deberá facilitarse de *"forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo"* y, a grandes rasgos, comprenderá:

- identidad y datos de contacto del **responsable** y, en su caso, de su representante;
- datos de contacto del **delegado de protección de datos**, en su caso;
- **fines y base jurídica** del tratamiento
- **destinatarios** o categorías de destinatarios;
- **transferencias a terceros países**
- **plazo de conservación** o, si no es posible, criterios utilizados para determinarlo;
- **derechos** (acceso, rectificación, supresión, limitación, oposición, portabilidad, retirar el consentimiento y presentar una reclamación ante la autoridad de control)
- si es **obligatorio facilitar** los datos, en particular si es un requisito legal o contractual o un requisito necesario para suscribir el contrato, y consecuencias de no hacerlo;
- existencia de **decisiones individuales automatizadas**; y
- si los datos no se obtienen del interesado: **categorías de datos y procedencia**.

Para facilitar esta tarea, la AEPD, en su Guía para el cumplimiento del deber de informar[5], recomienda facilitar la información por capas, incluyendo la información básica de forma resumida en una primera capa, y la información detallada en una segunda capa.

En particular, y dado su posible impacto en el ámbito de la publicidad online, donde es frecuente la realización de perfiles para remitir comunicaciones personalizadas, es importante destacar que las empresas que tomen **decisiones automatizadas que produzcan un efecto significativo** en los interesados (a las cuales ya nos hemos referido más arriba) deberán informar sobre la existencia de estas decisiones, ya que el RGPD obliga a proporcionar información sobre la lógica aplicada y la importancia y consecuencias previstas para el interesado.

[5] Disponible en: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf.

04

REALIZAR UNA EVALUACIÓN DE IMPACTO

Cuando sea probable que el tratamiento de datos previsto entrañe un alto riesgo para los derechos y libertades de los interesados, la empresa deberá realizar previamente una evaluación de impacto de las operaciones de tratamiento en la protección de datos personales. Por ejemplo, se entiende que existe un alto riesgo cuando se traten a gran escala categorías especiales de datos o cuando se haga una evaluación sistemática y exhaustiva de aspectos personales basada en un tratamiento automatizado y sobre cuya base se tomen decisiones con efectos jurídicos para los interesados.

Este análisis deberá documentarse y, a grandes rasgos, incluirá:

- la descripción de las operaciones y los fines del tratamiento;
- una evaluación de la necesidad y proporcionalidad de las operaciones;
- una evaluación de los riesgos para los derechos y libertades de los interesados; y
- las medidas previstas para afrontar esos riesgos.

Si, pese a la aplicación de las medidas, siguiera existiendo un riesgo residual alto, la compañía deberá **consultar a la autoridad de protección de datos** para que se pronuncie al respecto.

El GT29, en sus directrices de 4 de abril de 2017[6] (revisadas y adoptadas el 4 de octubre de 2017), recoge una lista de

[6] Disponibles en: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

posibles **factores de riesgo** y señala que, ante la concurrencia de dos o más de estos factores, el riesgo podrá considerarse alto y, por tanto, tendrá que realizarse la evaluación de impacto. Entre esos factores se incluyen:

- el tratamiento de datos de personas vulnerables (por ejemplo, menores);
- la adopción de decisiones automatizadas con efectos significativos;
- la monitorización sistemática;
- la combinación de bases de datos; y
- el uso de tecnologías innovadoras.

Por lo tanto, **habrá campañas publicitarias que requieran la realización de esta evaluación de impacto, especialmente en el ámbito de la publicidad online.** Las empresas deberán valorar cada campaña desde el momento de su concepción para determinar, conforme a sus circunstancias específicas, la necesidad de realizar este análisis.

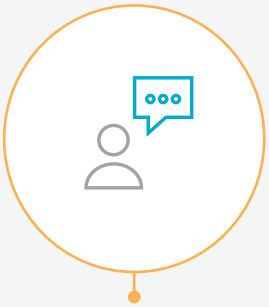
Antes de hacer una campaña de publicidad, especialmente online, se deberá valorar la necesidad de hacer una evaluación de impacto

05

OTRAS CUESTIONES A TENER EN CUENTA

OTRAS CUESTIONES RGPD

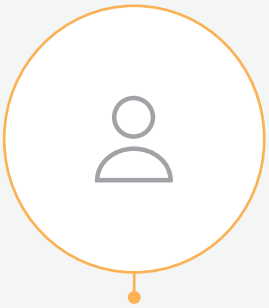
DERECHOS NUEVOS USUARIOS



VELAR POR LOS ENCARGADOS DE TRATAMIENTO

LLEVANZA DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO

MEDIDAS DE SEGURIDAD ADECUADAS AL RIESGO



DELEGADO DE PROTECCIÓN DE DATOS

SANCIONES: 20M O 4% VOLUMEN NEGOCIO TOTAL ANUAL

DERECHOS DE LOS INTERESADOS

La empresa deberá atender nuevos derechos, como el derecho a la limitación del tratamiento y el derecho a la portabilidad de los datos. Además, en el ámbito de la actividad publicitaria hay que atender los derechos a:

- oponerse al tratamiento con fines de mercadotecnia directa, incluida la elaboración de perfiles; y
- no ser objeto de una decisión automatizada con efectos significativos.

ENCARGADOS DE TRATAMIENTO

El RGPD otorga mayor importancia a la selección de encargados del tratamiento al exigir al responsable que solamente elija a aquellos prestadores de servicios que le ofrezcan garantías suficientes de adecuación a esta normativa.

Asimismo, el RGPD establece nuevas obligaciones para los encargados del tratamiento, así como el contenido mínimo del contrato de encargo de tratamiento, exigiendo mayor grado de detalle que la LOPD[7].

Las empresas deberán tener estos requisitos en cuenta en la negociación y elaboración de contratos entre anunciantes y agencias de publicidad cuando los servicios prestados por estas conlleven el tratamiento de datos personales de los destinatarios de la publicidad por cuenta del anunciante.

REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

El RGPD establece la obligación de llevar un registro por escrito de las actividades de tratamiento, en general para empresas de más de 250 empleados.

Este registro deberá mantenerse a disposición de las autoridades de protección de datos, para su supervisión de las operaciones de tratamiento. Por el contrario, ya no será necesario notificar ficheros para su inscripción en el Registro General de Protección de Datos.

[7] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)

MEDIDAS DE SEGURIDAD

A diferencia del RLOPD[8], que especifica las medidas de seguridad mínimas exigibles a responsables y encargados del tratamiento (divididas en tres niveles: básico, medio y alto, en función de la naturaleza de los datos), el RGPD señala, de forma genérica, que las medidas de seguridad deberán ser adecuadas al riesgo.

Para realizar esta valoración las empresas deberán tener en cuenta factores tales como la naturaleza, alcance, contexto y fines de tratamiento, el estado de la técnica, los costes de aplicación, y los riesgos para los derechos y libertades de los interesados.

NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

En caso de que se produzca cualquier violación de seguridad[9], el RGPD obliga a la compañía a notificar a la autoridad de protección de datos en el plazo máximo de 72 horas desde su detección, salvo que sea improbable que constituya un riesgo para los derechos y libertades de los interesados.

Estas incidencias también deberán comunicarse a los interesados sin dilación indebida, cuando sea probable que entrañen un alto riesgo para sus derechos y libertades, si bien se prevén algunas excepciones (por ejemplo, que se hayan tomado medidas con posterioridad que garanticen que ese alto riesgo no se materialice).

DELEGADO DE PROTECCIÓN DE DATOS

El RGPD introduce una nueva figura: el delegado de protección de datos o data protection officer, que es aquella persona designada por el responsable (o el encargado del tratamiento) para supervisar el cumplimiento de la normativa de protección de datos y asesorar en todos los aspectos relacionados con esta materia.

Su designación es obligatoria para las autoridades públicas, así como para empresas:

[8] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD)

[6] El RGPD entiende por violación de seguridad aquella que "ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".

- empresas cuya actividad principal implique un tratamiento de datos a gran escala que requiera la observación habitual y sistemática de los interesados; y
- empresas cuya actividad principal suponga un tratamiento a gran escala de categorías especiales de datos o de datos relativos a condenas e infracciones penales.

El delegado de protección de datos debe tener conocimiento especializado del Derecho y la práctica de protección de datos, disponer de recursos suficientes para cumplir sus funciones y gozar de independencia en el desempeño de sus funciones. Rendirá cuentas al más alto nivel jerárquico.

Aunque para ejercer como delegado de protección de datos no es obligatoria una certificación específica, la AEPD, en colaboración con la Entidad Nacional de Acreditación, presentó el pasado 13 de julio de 2017 el Esquema de certificación de delegados de protección de datos[7], para ofrecer mayor seguridad y fiabilidad a aquellas entidades que incorporen a esta figura en sus organizaciones.

SANCIONES

Las empresas se someten a importantes sanciones en caso de infracción. Frente a la multa de hasta 600.000 euros prevista para las infracciones muy graves en la LOPD, el RGPD establece multas de hasta 20 millones de euros o el 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la mayor cuantía.

[7] Disponible en: http://www.agpd.es/portalwebAGPD/temas/certificacion/common/pdf/ESQUEMA_AEPD_DPD.pdf

06

PRÓXIMOS PASOS

Los numerosos cambios introducidos por el RGPD obligan a las empresas a elaborar una hoja de ruta con las tareas a realizar para adecuarse a la nueva norma, estableciendo prioridades en función de los riesgos.

HOJA DE RUTA
PARA LA ACTIVIDAD PUBLICITARIA

- Revisar las cláusulas informativas sobre protección de datos para adecuarlas a los requisitos del RGPD.
- Comprobar si las bases de datos utilizadas con fines de marketing pueden seguir utilizándose; en particular, si los consentimientos obtenidos en su momento cumplen las condiciones del RGPD o si el tratamiento con estos fines puede ampararse en otra base jurídica, como el interés legítimo.
- Valorar si es necesario realizar evaluaciones de impacto de campañas publicitarias u otras acciones comerciales durante la fase de diseño de las mismas y, en su caso, llevarlas a cabo.
- Revisar y adecuar al RGPD los contratos de encargo de tratamiento (por ejemplo, entre anunciantes y agencias de publicidad).
- Realizar acciones formativas para que todo el personal que trate datos personales sea consciente de las implicaciones que la nueva normativa tiene en su trabajo, en particular los equipos de marketing.

SOBRE AUTOCONTROL

AUTOCONTROL es el organismo independiente de autorregulación de la industria publicitaria en España. Constituido en 1995 como asociación sin ánimo de lucro, está integrado por anunciantes, agencias de publicidad, medios de comunicación y asociaciones profesionales y su objetivo es trabajar por una publicidad responsable: veraz, legal, honesta y leal.

En este momento cuenta con más de 500 miembros directos y 2.000 indirectos.

Si quiere más información, puede ponerse en contacto con nosotros en digital@autocontrol.es.

Esta guía es orientativa y no pretende sustituir o constituir asesoramiento en esta materia

AUTOCONTROL
Asociación para la Autorregulación de la Comunicación Comercial

C/ Principe de Vergara 109, 5ª planta - 28002 Madrid

+34 91 309 66 37 | +34 91 402 50 80

digital@autocontrol.es

www.autocontrol.es