World Federation of Advertisers

Hunton & Williams

GDPR Guia para Marketeros

Cinco cosas que cada propietario de marca debe saber sobre el Reglamento General de Protección de Datos.

Aanda
Asociación Nacional de Avisadores de Chile

Sumario Ejecutivo

A partir de mayo de 2018, el Reglamento general de protección de datos (GDPR) exigirá que todas las empresas realicen cambios importantes en la forma en que recopilan y procesan los datos de los consumidores. Es probable que esto tenga un impacto significativo en los especialistas en marketing que utilizan datos de los consumidores para impulsar campañas de marketing específicas y eficaces. GDPR se aplica a cualquier empresa que ofrezca bienes o servicios a consumidores en la Unión Europea o supervisa el comportamiento de las personas en Europa. Esto significa que la mayoría de las compañías globales se verán afectadas, incluso si sus sedes mundiales no tienen sede en Europa. Las empresas podrían enfrentar grandes multas si no cumplen. Estas multas podrían alcanzar hasta el 4% de la facturación global anual de una empresa, lo que para las empresas Global 500 podría significar multas que van desde $ 800 millones hasta tan alto como $ 19,2 mil millones.

En una encuesta de 2017 de miembros de WFA, el 94% de las empresas que representaban más de 20 mil millones de dólares estadounidenses de gasto publicitario global dijeron que GDPR era importante para su organización. Sin embargo, el 70% dijo que los especialistas en marketing de su organización no estaban completamente al tanto de las implicaciones del GDPR para futuras campañas de marketing. Esta guía, desarrollada con el apoyo de Hunton & Williams LLP, tiene como objetivo ayudar a abordar esta brecha al resaltar cinco áreas clave de GDPR que los especialistas en marketing deben conocer para poder prepararse.

"GDPR es de vital importancia para nuestra empresa, ya que tendrá un impacto en nuestras operaciones globales en todo el mundo. Philips está invirtiendo recursos significativos para cumplir con los requisitos de GDPR y ayudar a los especialistas en marketing a comprender las implicaciones para su trabajo diario.

Blake Cahill, Vicepresidente Senior de Marketing Digital Global Y medios, PHILIPS

Contenidos

Sobre este documento

Acerca de este documento El Reglamento General de Protección de Datos (GDPR) es una pieza importante de regulación de la privacidad. Se aplicará a partir del 25 de mayo de 2018. Es probable que tenga un impacto significativo en casi todas las grandes multinacionales, ya que se aplica a cualquier empresa que ofrezca bienes o servicios a los consumidores en la UE o monitorea el comportamiento de las personas en Europa. Se podría requerir que estas compañías cambien sustancialmente la forma en que recopilan y usan los datos del consumidor. Desde la perspectiva de un propietario de marca, GDPR requerirá un mayor enfoque sobre cómo las marcas se comunican con los consumidores acerca de su privacidad y podría limitar la forma en que se pueden usar algunos datos del consumidor para desarrollar un marketing personalizado.

La Guía GDPR para Promotores de WFA destaca algunos de los elementos clave de GDPR son probablemente tenga un impacto en los propietarios de las marcas y brinde sugerencias concretas sobre cómo los especialistas en marketing deberían pensar sobre su enfoque de la privacidad en el contexto de GDPR. Si bien esta guía no es exhaustiva, el objetivo es resaltar algunas áreas donde los especialistas en marketing pueden comenzar a pensar en nuevos enfoques y comenzar discusiones con los expertos técnicos relevantes en sus organizaciones (por ejemplo, cumplimiento y gobierno digital) para conocer más acerca del enfoque de su compañía a GDPR. Esta guía pretende complementar, en lugar de sustituir o constituir, el asesoramiento legal.

¿Por qué es importante GDPR para los profesionales del marketing?

1. GDPR cambiará significativamente cómo y cuándo las empresas pueden utilizar los datos de consumo.

Europa a menudo se ve como una región con algunas de las normas más estrictas de protección de datos en el mundo y GDPR confirma esa imagen mediante el fortalecimiento de las protecciones de privacidad existentes para los consumidores. Esto incluye un enfoque mucho más fuerte para obtener el consentimiento significativo de los consumidores para usar sus datos personales, incluidos los estrictos requisitos para que las empresas mejoren la forma en que explican a los consumidores cómo se usarán sus datos.

2. GDPR afectará a casi todas las grandes compañías multinacionales.

GDPR se aplica a cualquier empresa que ofrezca bienes o servicios a consumidores en la UE o monitores de comportamiento de las personas en Europa.

Esto significa que la mayoría de las compañías globales se verán afectadas, incluso si sus sedes mundiales no están en Europa

3. Las empresas corren el riesgo de pagar grandes multas por incumplimiento.

Las sanciones por no cumplir con GDPR incluyen multas que podrían llegar hasta el 4% de la facturación global anual de una empresa. Para las empresas Global 500, esto podría significar multas que van desde $ 836 millones hasta tan alto como $ 19,2 mil millones. Además de las multas regulatorias, GDPR también abre la posibilidad de que los consumidores y las organizaciones sin fines de lucro inicien acciones legales para obtener una compensación en caso de procesamiento de datos en violación de GDPR.

Próximos pasos:

- Revise los activos digitales con información legal y, cuando sea necesario, actualice todos los puntos de contacto del consumidor para reflejar las nuevas reglas de consentimiento.
- Revise las prácticas de recopilación de datos de agencias y otros terceros para evaluar el cumplimiento con GDPR.

02

¿Qué pasa si el consentimiento no es una opción?

El consentimiento no es el único motivo legal en el que las empresas pueden confiar para el procesamiento de los datos personales. GDPR también permite que los datos personales se procesen, cuando sea necesario, para los intereses legítimos de la empresa sin necesidad de obtener el consentimiento. Esto puede ser particularmente relevante en casos donde obtener el consentimiento de un consumidor no sería una opción viable, por ej. porque la empresa no tiene un vínculo directo con el consumidor para pedir su consentimiento. Por ejemplo, en algunos casos, una empresa puede argumentar que tiene un interés legítimo en procesar los datos de un cliente, siempre que exista una relación relevante y apropiada entre ellos. Sin embargo, para confiar en el interés legítimo, los especialistas en marketing necesitarían trabajar con sus equipos legales para llevar a cabo una evaluación de riesgos legales que tenga en cuenta:

- El equilibrio entre el interés legítimo de la compañía y el derecho del consumidor a la privacidad (u otros derechos fundamentales).
- Si un consumidor esperaría razonablemente que sus datos personales se procesaran en esta situación, en función de su relación con la empresa.

Cuando las empresas procesen datos basados en 'interés legítimo', deberán explicar esos intereses a los consumidores (por ejemplo, en la política de privacidad de la compañía). Los profesionales del marketing deberían trabajar con sus equipos legales para explorar si un interés legítimo podría ser una base legal posible para el procesamiento de datos en ciertas situaciones.

Próximos pasos:

- Revise caso por caso con los equipos legales si se necesita el consentimiento para usar los datos recopilados a través de campañas de marketing.

03

Transparencia

La transparencia es uno de los principios clave de la legislación de protección de datos de la UE y GDPR introduce obligaciones adicionales de transparencia para las empresas. Requiere que las empresas brinden información a los consumidores sobre muchos elementos de cómo WFA de los anunciantes porque están usando (o están planeando usar) sus datos personales. GDPR también establece que la información sobre el procesamiento de datos debe proporcionarse de forma concisa e inteligible, utilizando un lenguaje claro y sencillo.

01

Consentimiento

GDPR se enfoca fuertemente en empoderar a los consumidores para que decidan cómo sus datos personales son utilizados por las empresas. El consentimiento ya es uno de varios motivos legales en los que las empresas pueden confiar para justificar el procesamiento de datos personales. Sin embargo, GDPR establece nuevas y amplias condiciones para que el consentimiento sea válido. Esto probablemente signifique que en muchos casos los consumidores necesitarán solicitar su consentimiento con más frecuencia, porque se necesitará consentimiento de ellos para cada propósito para el cual una compañía necesite procesar su información personal.

Además, los consumidores deberán recibir la posibilidad de retirar el consentimiento en cualquier momento.
Estos requisitos pueden afectar la experiencia en línea del consumidor y conducir a irritación o, en algunos casos, negativa a dar su consentimiento. En muchos casos, sin embargo, puede que ya no sea suficiente confiar en un permiso general dado marcando una casilla al registrarse en un servicio. Según las nuevas reglas, el consentimiento debe ser libremente específico informado y dado inequívoco, proporcionado ya sea por una declaración o una clara acción afirmativa.

Dado libremente	Los consumidores no pueden ser obligados a dar su consentimiento para que sean recogidos y procesados, a fin de firmar los datos necesarios para el servicio hasta un servicio, a menos que los datos funcionen.
Específico	En muchos casos, ya no será suficiente contar con el permiso otorgado marcando una casilla vinculada a una política de privacidad que cubra una amplia gama de usos de datos. Los consumidores también deberán acordar específicamente ciertos usos de sus datos.
Informado	Las compañías necesitarán proporcionar a los consumidores grandes cantidades de información sobre cómo son sus datos. Para obtener más información consulte el capítulo 3: Transparencia.
Inequívoco	El consentimiento de transparencia debe ser una indicación clara de que un el consumidor está aceptando que se usen sus datos. Es poco probable que algunos métodos pasivos de consentimiento (por ejemplo, seguir utilizando un sitio web sin leer el aviso de privacidad) se consideren inequívocos y suficientes.

Las marcas deberán ser capaces de demostrar que el consentimiento fue proporcionado de una manera que cumpla con estas condiciones, incluso si los datos fueron recopilados por un tercero. Esto significa que los marketers de la marca y sus equipos legales deberán trabajar con los socios de la agencia y otros terceros para garantizar que esto sea posible. En la mayoría de los casos, será necesario el consentimiento explícito para llevar a cabo cualquier tipo de perfil detallado del cliente. El consentimiento explícito significa que los consumidores deben tener la posibilidad de estar de acuerdo o en desacuerdo con un uso particular de todos sus datos personales al hacer una declaración afirmativa clara (escrita u oral).

También se requerirá el consentimiento explícito para procesar lo que GDPR llama "categorías especiales" de datos, que se consideran especialmente sensibles. Esto incluye:

- Datos personales que revelan origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, o sindicato membresía, a gran escala .
- Genetic2 o datos biométricos que identifican a una persona de manera única.
- Datos relacionados con la vida sexual u orientación sexual de salud.
- Datos relacionados con condenas y delitos penales.

Estos requisitos crean un difícil acto de equilibrio para los especialistas en marketing. Por un lado, se debe proporcionar más información a los consumidores, pero debe hacerse de una manera que no sea abrumadora o difícil de entender. Los profesionales del marketing necesitarán explorar formas creativas de incorporar esto en campañas digitales basadas en datos. En febrero de 2017, wFA dirigió un taller de Intercambio de Gobernanza Digital (DGX) para miembros para compartir ideas y mejores prácticas sobre cóm,o, dónde y cuándo se debe obtener el consentimiento para crear las mejores condiciones para que los consumidores tengan transparencia, elección y control sobre sus datos personales. Seis principios clave surgieron durante la sesión, que pueden ser útiles cuando se piensa en cómo implementar este elemento de GDPR.

MANTÉNGALO VISUAL	La idea de 'emoji' utiliza símbolos fáciles de entender para explicar las políticas de privacidad, p. sellos, marcas de confianza, íconos. Cuéntame una historia de videos cortos en lugar de texto.
MANTÉNGALO CORTO Y SIMPLE	Usa solo el lenguaje que un niño de 13 años podría entender. Manténlo relevante Resalta lo que es notable y permite que los usuarios hagan clic para leer más.
NO ME ENGAÑE	Solo pide consentimiento cuando sea necesario. Se no intrusivo no se interponga en el camino de la experiencia del usuario.
DEJAME CAMBIAR MI MENTE	Recupere el control. Cree sistemas fáciles de usar que permitan a los usuarios controlar todas sus configuraciones de privacidad en un solo lugar, por ejemplo tableros, centros de notificación, botón de lamentar las barras de tareas ofrecen a los usuarios la posibilidad de volver a ingresar y salir fácilmente cuando lo deseen.
HÁGALO FÁCIL	Salir de la situación más fácil y rápido que entrar. Gestos fáciles para activar o desactivar, por ejemplo, deslizar en lugar de hacer clic
DIME LO QUE VAS A HACER	Explicar usuarios por qué quiere su información cuando se los piden Explicar las consecuencias / implicaciones de decir sí o no. Explicar claramente el intercambio de valores, por ejemplo, 1 video musical, 10 segundos de anuncio

Próximos pasos

Explore formas creativas de generar información sobre privacidad en campañas de marketing en línea y activos digitales.

04

Procesamiento de datos de los niños

Para procesar datos personales relacionados con niños, se requiere el consentimiento de los padres GDPR establece la edad de un niño "menor de 16 años", aunque los reguladores nacionales en los países de la UE puede optar por reducir esta edad a entre 13 y 16 años Esto significa que las empresas necesitarán establecer mecanismos para solicitar y verificar el consentimiento de los padres Aunque los reguladores nacionales en algunos países de la UE decidan reducir la edad a la que se da el consentimiento de los padres necesario, las empresas deben estar preparadas para seguir los pasos para implementar estos mecanismos para niños hasta la edad de 16 años.

GDPR no proporciona detalles específicos sobre cómo verificar que el consentimiento de los padres sea válido. Inicialmente, las empresas que tienen servicios o productos que atraen principalmente a los niños pueden desear movilizar sus departamentos legales o de asuntos públicos para que se relacionen con la autoridad de protección de datos en su jurisdicción a fin de solicitar orientación sobre cómo implementar estas medidas.

Próximos pasos
Revise todas las campañas y / o activos digitales que pueden implicar el uso de datos de niños (menores de 16 años), ya que es posible que se requiera el consentimiento de los padres.

05

Procesamiento de datos de los niños

En muchos casos, los datos personales se recopilan con un propósito específico en mente, p. como inscribirse para recibir un boletín de noticias. Sin embargo, los especialistas en marketing podrían estar interesados en utilizar esta información para desarrollar ideas que podrían ser utilizadas en otras campañas de marketing o para la orientar mensajes similares sobre todo en otros productos o servicios. GDPR solo lo permite bajo circunstancias específicas. Si no es posible (o apropiado) pedir nuevamente al consumidor su consentimiento, los especialistas en marketing necesitarán trabajar con sus equipos legales para llevar a cabo una evaluación de si los datos pueden usarse para otros fines sin consentimiento.

Esta evaluación deberá tener en cuenta:

- Cualquier vínculo entre los propósitos para los cuales los datos fueron originalmente recolectados y para lo que los mercadólogos desearían utilizar en el futuro.
- El contexto en el que se recopilaron originalmente los datos.
- Las expectativas razonables de los consumidores, en función de su relación con la empresa.
- Si los datos son 'sensibles'.
- Las posibles consecuencias de usar esta información para nuevos propósitos.
- Si los datos han sido anonimizados, encriptados o protegidos de otras maneras.

Próximos pasos
Cuando desee reutilizar los datos recopilados de campañas históricas, hable con su equipo legal para verificar si esto aún es posible.

Checklist

Cuando se aplique GDPR en todos los países de la UE el 25 de mayo de 2018, los especialistas en marketing deberán estar preparados para los cambios destacados en esta guía. Para prepararse, los especialistas en marketing deberían considerar tomar al menos los siguientes pasos:

* Explorar formas creativas de compilar información sobre privacidad en campañas de marketing en línea y activos digitales.
* Revisar los activos digitales con legal y, cuando sea necesario, actualizar todos los puntos de contacto del consumidor para reflejar las nuevas reglas de consentimiento.
* Revise todas las campañas y / o activos digitales que puedan implicar el uso de datos de niños (menores de 16 años) ya que se puede requerir el consentimiento de los padres.
* Revisión caso por caso con los equipos legales si se necesita el consentimiento para utilizar los datos recopilados a través de campañas de marketing.
* Al intentar reutilizar los datos recopilados de las campañas históricas, hable con su equipo legal para verificar si esto aún es posible.
* Revisar las prácticas de recopilación de datos de agencias y otros terceros para evaluar el cumplimiento con GDPR.

Consideraciones adicionales

La siguiente sección analiza una serie de otros elementos de GDPR que, aunque es probable que tengan un menor impacto directo en los especialistas en marketing, son útiles para tener en cuenta desde una perspectiva empresarial.

Para obtener más información sobre cómo su organización se prepara para implementar los siguientes requisitos, le sugerimos que se comunique con sus equipos legales.

Responsabilidad

GDPR requiere que las empresas implementen un número de medidas para poder demostrar cierto grado de cumplimiento, incluidas las siguientes:

Se requerirá que algunas compañías designen un Oficial de Protección de Datos (DPO) para supervisar todas las actividades de procesamiento de datos. Este requisito solo se aplica a las empresas cuyas actividades principales implican:

* Monitorear regularmente a las personas de manera sistemática a gran escala.
O
* Procesar datos personales que revelen origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, o membresía sindical, “a gran escala”.
O
* Procesamiento de datos genéticos o biométricos para identificar de manera única a una persona, "a gran escala" .
O
* Procesamiento de datos relacionados con la salud, la vida sexual o la orientación sexual, "a gran escala".
O
*Procesamiento de datos relacionados con condenas y delitos penales, "a gran escala".

Las empresas deberán evaluar si se ajustan a alguna de las categorías anteriores para decidir si están legalmente obligadas a nombrar un oficial de protección de datos.

Las compañías necesitarán establecer un sistema interno para llevar a cabo evaluaciones de impacto de protección de datos antes de hacer cualquier procesamiento de datos que probablemente genere un alto riesgo de privacidad para los individuos. Los mercadólogos deben trabajar con sus equipos legales para comprender cómo y cuándo activar una evaluación de impacto de protección de datos para los próximos proyectos.

Las empresas deberán mantener registros internos de sus actividades de procesamiento por escrito, aunque las compañías con menos de 250 empleados pueden estar exentas (bajo ciertas condiciones). GDPR proporciona una lista de la información que necesitaría ser incluido en estos registros. Las empresas sin una base de la UE deberán nombrar a un representante de la UE en un único país de la UE que actuará como punto de contacto para las autoridades de protección de datos.

Derechos del consumidor

Las empresas deberán asegurarse de que se establezcan sistemas para responder a las solicitudes de los consumidores sobre sus datos personales. Los consumidores tendrán derecho a solicitar a las empresas que les den acceso a sus datos y solicitar que se eliminen, corrijan o modifiquen (sujeto a ciertas condiciones).

Los consumidores también tendrán derecho, bajo ciertas condiciones, a oponerse al procesamiento de sus datos personales y que se les devuelvan sus datos personales. También pueden solicitar que sus datos sean transferidos a otra compañía. Las empresas deberán estar preparadas para responder a estas solicitudes "sin demoras innecesarias y actualizar sus sistemas de TI en consecuencia".

Notificaciones de violación de datos

Cualquier incidente de seguridad relacionado con datos personales (como un hack o una fuga) se notificará en 72 horas a la autoridad de protección de datos correspondiente. En algunos casos, también será necesario notificar a los consumidores directamente. El breve plazo de notificación exigirá que las empresas respondan muy rápidamente a cualquier sospecha de incidentes de seguridad relacionados con los datos personales y podría tener implicaciones para la reputación de la marca.

Los profesionales del marketing deben considerar trabajar con áreas legales, de TI y otras partes del negocio para desarrollar una estrategia de comunicación estándar para responder a los incidentes de seguridad relacionados con los datos personales. Esto podría implicar el desarrollo de técnicas e ideas sobre cómo notificar a los consumidores directamente con un daño mínimo a la reputación de la marca.

Sanciones

Las empresas enfrentarán multas de hasta el 4% de la facturación anual global 13 o 20 millones de euros14 por incumplimiento de GDPR, el que sea mayor.

Los consumidores, las organizaciones sin fines de lucro y las asociaciones que representan a los consumidores también podrán iniciar procedimientos legales contra las empresas por el incumplimiento de GDPR.

Información de contacto

Póngase en contacto con Catherine Armitage, Gerente Senior de Asuntos Públicos, para obtener más información (c.armitage@wfanet.org +32 470 367677).

[1]Monitoreo "se refiere, por ejemplo, al rastreo de individuos en línea.

[2]Los datos genéticos se definen en GDPR como" todos los datos personales relacionados con las características genéticas de un individuo que brindan información única sobre la fisiología o la salud de ese individuo ".

[3]Definido en GDPR como "cualquier dato personal relacionado con las características físicas, fisiológicas o de comportamiento de un individuo que permita o confirme la identificación única de ese individuo", por ejemplo, imágenes faciales o datos dactiloscópicos (huellas dactilares)

[4]Los datos relativos a la salud se definen en GDPR como " datos personales relacionados con la salud física o mental de un individuo que revelan información sobre su estado de salud. "Esto incluye información sobre la prestación de servicios de salud.

[5]Para obtener más información sobre el concepto de" interés legítimo ", consulte el Artículo 29 Protección de datos El dictamen del Grupo de Trabajo 6/2014 sobre la noción de intereses legítimos del centro de datos

[6]A menos que se puedan dar otros motivos legales usado, vea el Capítulo 2: ¿Qué pasa si el consentimiento no es una opción?

Los datos biométricos se definen en GDPR como "cualquier dato personal relacionado con las características físicas, fisiológicas o de comportamiento de un individuo que permite o confirma la identificación única de ese individuo", p. datos de imágenes faciales o dactiloscópicas (huellas dactilares).

[8]Los datos relativos a la salud se definen en GDPR como" datos personales relacionados con la salud física o mental de un individuo que revelan información sobre su estado de salud ".

[9]Esto incluye información sobre la prestación de servicios de salud. Además, las empresas También es necesario evaluar requisitos de OPD específicos que (continúen) aplicándose a nivel de los Estados miembros de la UE.

[10]Las empresas que no cumplan los criterios descritos en este documento no están obligadas a designar un OPD bajo GDPR, pero pueden querer designar un OPD de forma voluntaria para facilitar el cumplimiento de los requisitos de GDPR Este tipo de OPD voluntario estará sujeto a los mismos requisitos en GDPR que se aplican al designar un OPD es obligatorio.

[11]Se requerirán evaluaciones de impacto de protección de datos para cualquier procesamiento de datos que sea es probable que resulte en un alto riesgo para los derechos y libertades de las personas.
12GDPR define los incidentes de seguridad relacionados con los datos personales como "infracciones de datos e, violación de seguridad que conduce a la destrucción accidental o ilegal, pérdida, alteración, divulgación no autorizada y / o acceso a datos personales, transmitidos, almacenados o procesados.

[12]Del año anterior.

[13]Aproximadamente equivalente a USD 22,5 millones.

Nota: Todos los puntos de referencia, resultados de encuestas, agendas y actas de FA son revisados por Hogan Lovells International LLP, nuestros abogados de competencia.

Política de cumplimiento de leyes de competencia de WFA.

Hogan Lovells

El objetivo de WFA es representar los intereses de los anunciantes y actuar como foro de Hogan para contactos legítimos. entre los miembros de Lovells de la industria publicitaria.

El objetivo de WFA es representar los intereses de los anunciantes y actuar como foro de Hogan para contactos legítimos. entre los miembros de Lovells de la industria publicitaria. Es obvio que la política de la WFA es que no será utilizada por ninguna compañía para fomentar conductas anticompetitivas o colusorias, ni para involucrarse en otras actividades que puedan violar cualquier ley, reglamentación, regla o directivas antimonopolio o de competencia de cualquier país o de otra manera perjudicar la competencia plena y justa.

La WFA realiza controles regulares para asegurarse de que se cumpla estrictamente con esta política. Como condición de membresía los miembros de la WFA reconocen que su membresía en la WFA está sujeta a las normas de la ley de competencia y acuerdan cumplir plenamente con esas leyes. Los miembros acuerdan que no usarán la WFA, directa o indirectamente, (a) para alcanzar o intentar llegar a acuerdos o entendimientos con uno o más de sus competidores, (b) para obtener o intentar obtener, intercambiar o intentar intercambiar información confidencial o patentada sobre cualquier otra empresa que no sea en el contexto de un negocio de buena fe o (c) promover cualquier conducta anticompetitiva o colusoria, o participar en otras actividades que puedan violar cualquier ley antimonopolio o de competencia, regla de regulación o directivas de cualquier país o de otra manera perjudicar la competencia plena y justa.plena y justa. La WFA realiza controles regulares para asegurarse de que se cumpla estrictamente con esta política. Como condición de membresía los miembros de la WFA reconocen que su membresía en la WFA está sujeta a las normas de la ley de competencia y acuerdan cumplir plenamente con esas leyes.