PRIVACIDAD DE DATOS MARKETING

PRIVACIDAD DE DATOS EN MARKETING Y CUMPLIMIENTO: MEJORES PRÁCTICAS EN 2025

USERCENTRICS

Cuando los clientes te confían sus datos, parte crucial de tus estrategias de marketing y ventas, es tu deber respetar su privacidad y tratarlos de forma ética y legal.

De lo contrario, te arriesgas a sanciones y multas por incumplimiento, pérdida de confianza de los clientes y daños a tu reputación. Por eso es tan importante asumir la responsabilidad de la privacidad de los datos de marketing y garantizar el cumplimiento de las normativas y directrices pertinentes.

A medida que evoluciona la normativa, resulta difícil asegurarse de estar siempre al día sobre las mejores prácticas de cumplimiento y privacidad de datos. Aquí tienes recomendaciones que te ayudarán y herramientas que te facilitarán el proceso.

¿QUÉ ES LA PRIVACIDAD DE LOS DATOS EN MARKETING?

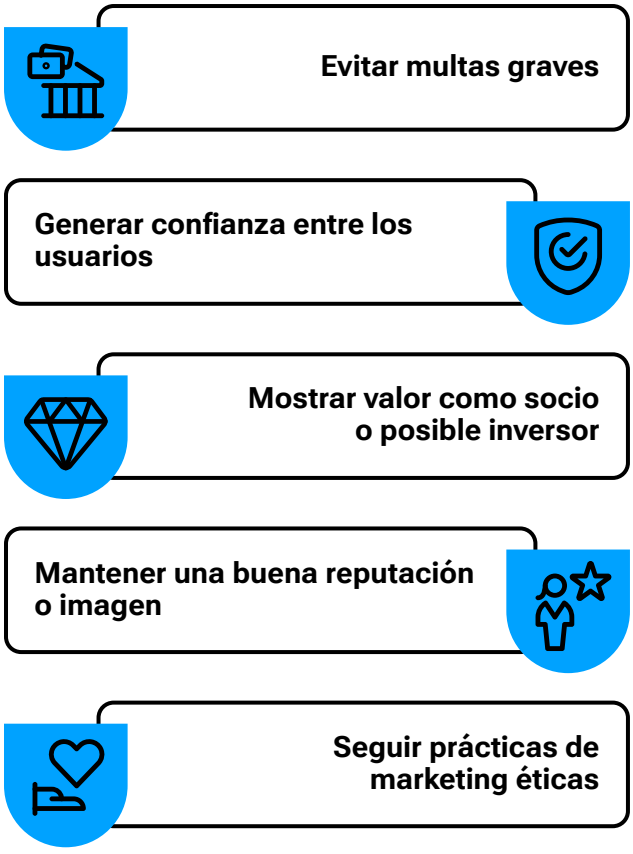
La privacidad de datos en marketing implica proteger la información personal de los individuos recopilada para permitir las actividades de marketing. Esto incluye el tratamiento ético y responsable de los datos en todas las actividades de marketing, así como el uso de tecnologías, políticas y estrategias para salvaguardar los datos de los usuarios.

Existen numerosas normativas sobre protección de datos en todo el mundo, y las empresas deben asegurarse de que cumplen todas las leyes pertinentes que les sean aplicables, lo que normalmente implica las leyes que protegen a los clientes y usuarios allí donde residen, no donde está ubicada la empresa.

Todas las partes implicadas en marketing deben ser responsables de ello de forma permanente, pero especialmente los jefes de los departamentos de marketing y ventas y, en algunos casos, un responsable de protección de datos.

Al dar prioridad a la privacidad de los datos y utilizar las herramientas adecuadas, estarás demostrando tu compromiso con la ética y las responsabilidades legales, generando confianza en los clientes y reduciendo los riesgos de incumplimiento, así como sanciones.

Por qué es importante la seguridad de los datos de los consumidores



Proteger los datos de los consumidores es vital por varias razones. El incumplimiento de las leyes y los requisitos de la política de privacidad puede suponer multas y otras sanciones legales. Sin embargo, proteger los datos no solo es cuestión de cumplir la ley, sino también de respetar a los usuarios, comportarse de forma ética y generar confianza y relaciones duraderas con unos consumidores cada vez más concienciados con la privacidad.

NORMATIVAS Y DIRECTRICES SOBRE PROTECCIÓN DE DATOS PARA EL SECTOR DEL MARKETING

La privacidad de datos en marketing es compleja, con multitud de normativas que varían según la región e incluso el sector o el tipo de actividad. Muchas empresas tienen que mantenerse al día y cumplir múltiples normativas, directrices y marcos de privacidad que son pertinentes para sus actividades de marketing.

Estas son algunas de las principales normas de protección de datos que se aplican:

- Reglamento General de Protección de Datos (RGPD)
- Ley de Mercados Digitales (DMA)
- Ley de Privacidad del Consumidor de California (CCPA) / Ley de Derechos de Privacidad de California (CPRA)
- Directiva ePrivacy (ePD)

Pero hay que tener en cuenta que existen muchas más normativas específicas de regiones y países, como la Ley Alemana de Protección de Datos de Telecomunicaciones y Telemedios (Telekommunikations-Telemedien-Datenschutzgesetz, TTDSG) y la Ley de Protección de Datos (Data Protection Act, DPA) del Reino Unido.

Saber más: Requisitos de consentimiento de la UE y la legislación sobre privacidad de datos: listado por países

Reglamento General de Protección de Datos (RGPD)

El RGPD entró en vigor en 2018. El documento contiene 88 artículos que regulan el uso y el tratamiento de los datos personales, así como la responsabilidad de mantenerlos a salvo. Cubre los datos de las empresas y los consumidores ubicados en los 27 países miembros de la UE y en otros tres países del Espacio Económico Europeo, independientemente de la sede del responsable del tratamiento.

El RGPD exige que todas las organizaciones que ofrezcan bienes o servicios a residentes en la UE y procesen datos personales cumplan el Reglamento, defiendan los derechos de privacidad de las personas y salvaguarden los datos personales recopilados y procesados. Hay siete principios que deben aplicarse y ocho derechos de privacidad de los consumidores que deben respetarse en virtud del RGPD.

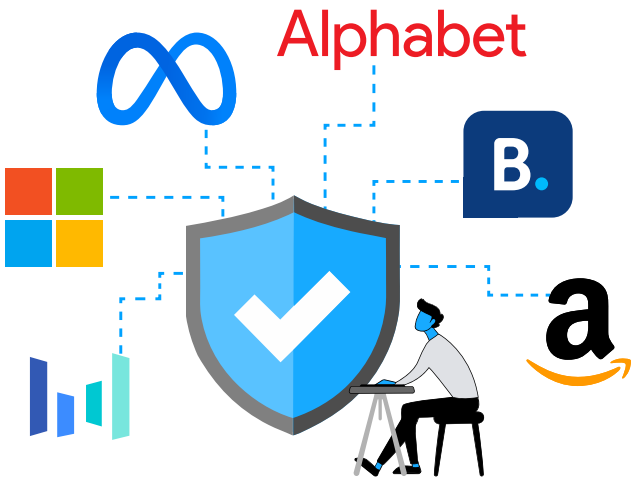
Ley de Mercados Digitales (DMA)

La Comisión Europea (CE) introdujo la DMA en 2022 para regular los mercados digitales, proteger la privacidad de los consumidores y equilibrar el terreno competitivo entre los grandes gigantes tecnológicos y las empresas más pequeñas.

Este marco regulador tiene como objetivo fomentar la competencia leal, mejorar la protección de los consumidores y promover el ecosistema digital mediante mejores prácticas de consentimiento de los usuarios y tratamiento de datos.

La DMA se centra en la regulación de las empresas designadas como «gatekeepers» por la ley. Esto afecta no solo a estas grandes empresas, sino también a las empresas más pequeñas que utilizan sus plataformas y servicios para sus ventas y marketing, como Google Ads. Para que los gatekeepers cumplan con las normas de privacidad de datos, sus clientes también deben cumplir con estos requisitos. Esto garantiza el cumplimiento de la privacidad en todos los ecosistemas de las plataformas de los gatekeepers:

- Microsoft (propietario de LinkedIn y Windows PC OS)
- Meta (propietario de Facebook, Instagram, WhatsApp, entre otros)
- Alphabet (propietario de Google, YouTube y Android)
- ByteDance (propietario de TikTok)
- Booking.com (añadido en mayo de 2024)
- Amazon (propietario de Amazon Marketplace)
- Apple (propietario de iOS y de App Store)



Ley de Privacidad del Consumidor de California (CCPA) / Ley de Derechos de Privacidad de California (CPRA)

Actualmente, en Estados Unidos no existe una ley federal unificada de protección de datos. Por lo tanto, cada estado ha ido aprobando sus propias leyes de privacidad. La primera fue la Ley de Privacidad del Consumidor de California, aprobada en 2018 y vigente desde 2020. Posteriormente, fue ampliada y modificada, siendo sustituida en 2023 por la Ley de Derechos de Privacidad de California.

Las leyes estatales de privacidad de datos protegen la información personal de sus residentes y se aplican a las empresas que operan dentro de sus fronteras. Actualmente, estas leyes adoptan un modelo de consentimiento de «opt-out» o exclusión voluntaria, lo que significa que las empresas pueden recopilar y utilizar datos de usuario sin su consentimiento previo. Sin embargo, deben proporcionar un enlace claro y visible en su sitio web, como «no vender ni compartir mi información personal», que permita a los usuarios rechazar el tratamiento de sus datos, la publicidad dirigida y la creación de perfiles.

Hasta la fecha, California es el único estado de EE.UU. que permite a los consumidores demandar a una empresa por daños y perjuicios derivados de una vulneración a través del derecho de acción privada. También es el único estado que ha creado una agencia que vela por el cumplimiento de las leyes y otras funciones, la Agencia de Protección de la Privacidad de California (CPPA). En todos los demás estados, esta tarea depende de la Fiscalía General, como ocurría en California hasta la entrada en vigor de la CPRA.

Directiva ePrivacy (ePD)

Esta ley engloba tanto la Directiva ePrivacy (ePD) como la propuesta de Reglamento ePrivacy. La ePD, también conocida como la «ley de cookies», aborda específicamente cuestiones de privacidad en la comunicación digital y se aplica en la UE. Las directrices actuales de la ePD deben aplicarse a nivel nacional en cada país de la UE.

Esta normativa estipula que la comunicación a través de redes públicas debe ser confidencial, exige el consentimiento del usuario para las cookies, regula las prácticas de marketing directo y establece directrices de seguridad para los servicios de comunicación digital.

6 CONSEJOS PARA RECOPILAR DATOS Y ALMACENARLOS DE FORMA SEGURA

Recopilar datos y cumplir la normativa no es tarea fácil, pero es esencial para desarrollar la actividad comercial al tiempo que se respeta al consumidor. Por ello, el Privacy-Led Marketing se está convirtiendo en la ventaja competitiva de las empresas.

Con tantas normativas y requisitos en vigor, ¿cuáles son algunas de las mejores prácticas para garantizar que los datos se recopilan y almacenan de forma ética? Aquí tienes seis consejos que deberías aplicar.

> *Prioriza el respeto de la privacidad de los datos y cuenta con asesores jurídicos cualificados y/o expertos en privacidad para que tu empresa pueda lograr y mantener el cumplimiento a medida que cambia el panorama tecnológico y jurídico. Esto también permitirá a tu empresa elaborar y actualizar políticas integrales que evolucionen con las leyes y las tecnologías, así como proteger los datos de la empresa, las operaciones de marketing y reforzar la seguridad ante terceros.*
>
> **Adelina Peltea**
> CMO de Usercentrics

1. Actualiza periódicamente la política de privacidad

Es fundamental que las organizaciones mantengan políticas de privacidad claras, precisas y exhaustivas en sus sitios web y aplicaciones. Estas políticas deben adaptarse a las estrategias de marketing específicas y al comportamiento del público objetivo.

Sin embargo, dado que las leyes y normativas están sujetas a cambios, es preciso que revises estas políticas periódicamente. Se trata de documentos legales dinámicos y su actualización continua es un componente esencial del proceso para asegurar tanto el cumplimiento normativo como la transparencia.

Además, es importante registrar la fecha de la última modificación y proporcionar acceso a las versiones anteriores.

Por ejemplo, una nueva operación de marketing puede requerir nuevos consentimientos para distintos tipos de recopilación de datos, o una campaña dirigida a una nueva región puede exigir el cumplimiento de normativas adicionales. Comunica claramente las actualizaciones a tus consumidores y asegúrate de que puedan optar fácilmente por no participar (si procede) si no están conformes con las nuevas acciones.

2. Obtén consentimiento informado durante la recopilación de datos

En muchas regiones, obtener consentimiento informado es imprescindible para el cumplimiento de la normativa, de modo que la privacidad en marketing se convierte en una prioridad.

Si sigues prácticas de recopilación basadas en la privacidad, es necesario obtener consentimiento explícito e informado antes de recopilar y utilizar los datos de origen. Asimismo, debes mantener registros de los datos recogidos y del consentimiento otorgado, además, los usuarios deben tener la posibilidad de cambiar o revocar su consentimiento en el futuro.

Si se retira el consentimiento, deberás cesar la recopilación y el tratamiento de datos lo antes posible y, entre otras acciones, deberás corregir o eliminar los datos si así lo solicita la persona de la que proceden. Los derechos específicos varían según las leyes de privacidad.

Saber más: Normativa sobre privacidad de datos por estados: derechos y requisitos

La primera interacción de un consumidor con un sitio web o una aplicación suele ser una solicitud de consentimiento, y causar una buena primera impresión es importante. Recopilar, almacenar y notificar el consentimiento de forma clara, transparente y precisa es esencial para no dificultar la experiencia de navegación de los consumidores.

Una plataforma de gestión del consentimiento (CMP) como Usercentrics CMP automatiza y agiliza el proceso de recopilación, almacenamiento y notificación del consentimiento, permitiéndote cumplir la normativa y proteger la privacidad de tus clientes.

3. Depura las listas de correo electrónico con frecuencia

La gestión ética y eficaz de las listas de correo electrónico es un componente fundamental de las responsabilidades de un profesional del marketing. No basta con dar el consentimiento una vez: hay que otorgarlo para cada nueva acción de marketing. El consentimiento también caduca, con plazos que varían según la normativa, lo que significa que tendrás que renovarlo periódicamente.

Los responsables del marketing por correo electrónico también deben garantizar que los datos personales sean exactos, estén actualizados y sean accesibles si un cliente desea rectificarlos, consultarlos o eliminarlos. En este sentido, el RGPD otorga a las personas derechos como el ***derecho de acceso*** (art. 15 del RGPD) y el ***derecho al olvido*** (art. 17 del RGPD).

Los profesionales del marketing deben facilitar a los consumidores la presentación de estas solicitudes y su aplicación, así como darse de baja. Las buenas prácticas de protección de datos también incluyen el uso de la doble confirmación de suscripción y la eliminación periódica de suscriptores inactivos e información obsoleta.

4. Desarrolla una conciencia ética

La protección de datos no consiste sólo en marcar casillas, sino que implica un cambio fundamental en la actitud de todos los profesionales del marketing respecto a la protección y ética de los datos. Se trata de comprender el valor de las estrategias de marketing basadas en la privacidad. Tienes que generar y mantener la confianza del cliente, y esto requiere responsabilidad por parte de las personas que recopilan datos personales de los consumidores.

Otro aspecto fundamental es la minimización de los datos: calidad frente a cantidad. En lugar de recopilar grandes cantidades de datos (a menudo de manera dudosa en el caso de algunos datos de terceros) recoge únicamente los datos que necesites para una actividad concreta y consérvalos solo el tiempo necesario para cumplir ese propósito. Céntrate en recopilar datos de origen cero y propios de calidad directamente del usuario para obtener información valiosa sobre tu público objetivo relevante.

5. Garantiza el control de la visibilidad de los datos

La privacidad de los datos no solo se trata de prevenir filtraciones externas mediante una mayor seguridad, sino también de proteger los datos dentro de la propia organización.

No todos los miembros de una organización necesitan tener acceso a los datos de los clientes, por lo que debes contar con sistemas que garanticen que sólo las partes relevantes y autorizadas puedan acceder a ellos con un fin específico.

Esto se aplica también a vendedores, proveedores, terceros y tecnologías como las plataformas de IA. En palabras de Adelina Peltea, CMO de Usercentrics:

> ***Los profesionales del marketing quieren romper los silos para obtener una visión de 360 grados de los consumidores, pero al mismo tiempo es importante limitar el acceso a los datos solo a quienes los necesitan específicamente y para funciones concretas.***

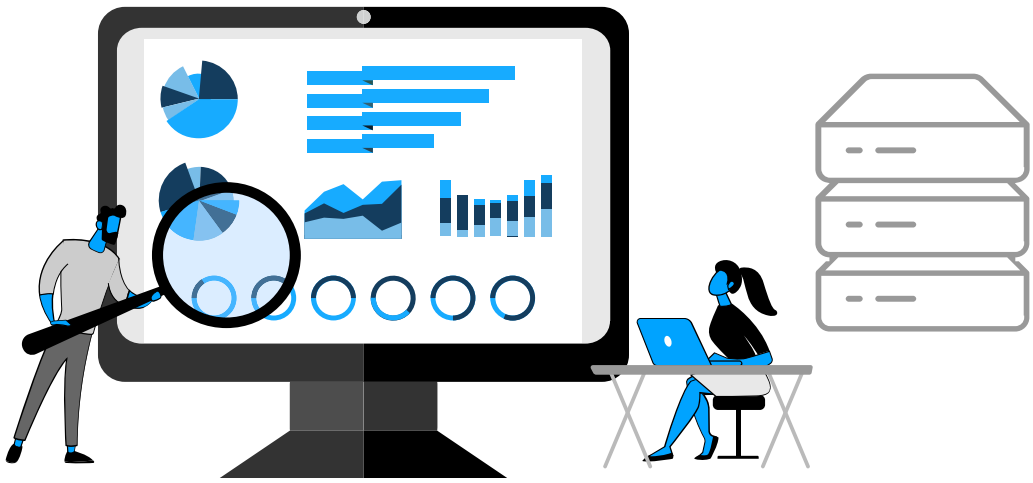
Por tanto, supervisa y actualiza periódicamente quién puede acceder a los datos, tanto interna como externamente, para seguir cumpliendo la normativa. Asimismo, los clientes también deben tener control sobre sus datos. En virtud de algunas leyes, deben poder acceder a sus datos y recibir una copia de los mismos, así como solicitar que se modifiquen o supriman.

6. Utiliza una plataforma de gestión del consentimiento (CMP)

Respetar la privacidad de los datos puede convertirse en una tarea compleja, lenta y estresante, ya que existen muchas normativas diferentes, cambios frecuentes en la legislación, diversos tipos de datos y distintos niveles de consentimiento.

> ***Cuantas más normativas y requisitos existen, mayores son las exigencias para las empresas, lo que puede resultar difícil de gestionar, especialmente para las organizaciones pequeñas con recursos limitados,*** afirma Peltea. ***Hay excelentes herramientas para ayudar a las empresas a gestionar los requisitos de manera automatizada, como las plataformas de gestión de consentimientos y los generadores de políticas de privacidad.***

Si utilizas una CMP como Usercentrics CMP, es más fácil almacenar los datos cedidos, gestionar y notificar el consentimiento a los socios de publicidad y análisis, y cumplir con las nuevas normativas. Todo ello ayuda a proteger tu negocio y te permite centrarte en mejorar tus campañas de marketing y aumentar tu cartera de clientes.



DESAFÍOS EN LA SEGURIDAD DE DATOS EN MARKETING

Garantizar la seguridad de los datos de marketing es una tarea compleja: es necesario mantenerse al día con las cambiantes regulaciones, mitigar riesgos, proteger los datos contra filtraciones y evitar que se compartan accidentalmente. A continuación, presentamos algunos de los errores más comunes y cómo prevenirlos.

> *Más normativas, más datos, más sistemas, más socios, más usos y más agentes malintencionados suponen más amenazas para el cumplimiento de la privacidad y la seguridad de los datos de las empresas. Para protegerse a sí mismas y a sus clientes, las empresas necesitan una gestión experta de las operaciones relacionadas con los datos y la privacidad, políticas y protocolos de seguridad sólidos, formación continua del personal y herramientas sólidas.*

Adelina Peltea
CMO de Usercentrics

Compartir datos de forma involuntaria

Los datos son más vulnerables cuando se descargan, almacenan o se hacen copias de seguridad sin conexión en soportes portátiles. Esto dificulta el almacenamiento seguro y la protección, así como el tratamiento coherente de los datos y la reducción de posibles errores humanos.

Los empleados pueden poner en peligro los datos de forma accidental, por ejemplo, extraviando dispositivos o siendo víctimas de robo. Además, los agentes malintencionados pueden acceder a los sistemas de la empresa mediante correos electrónicos de phishing.

Para reducir este riesgo, se puede limitar el acceso a los datos, aplicar políticas internas de almacenamiento y proporcionar formación continua a los empleados.

Filtraciones y accesos no autorizados

Las filtraciones son un peligro para cualquier empresa que recopile datos, y si se ven comprometidos, estos pueden ser borrados o vendidos ilícitamente. En caso de que se produzca una filtración de datos, puedes enfrentarte a multas y sanciones, así como al cese de las operaciones comerciales, la pérdida de clientes y una reputación dañada. En el ámbito del marketing, esto afecta tanto la capacidad de retención de clientes como la de generar nuevos contactos y socios comerciales.

Para evitar estas situaciones, actúa de forma proactiva y adopta políticas, procedimientos y medidas firmes de ciberseguridad para impedir que otras personas que no sean el responsable del tratamiento y los procesadores de datos autorizados puedan acceder a los datos de marketing. Al comunicar una filtración de datos a los clientes, hazlo lo antes posible, con empatía y transparencia. Intenta siempre mitigar los daños tanto como puedas.

GESTIONA EL CONSENTIMIENTO DE LOS USUARIOS Y CUMPLE LA NORMATIVA SOBRE PRIVACIDAD DE DATOS CON USERCENTRICS CMP

La privacidad de los datos es un aspecto fundamental que los profesionales del marketing no pueden pasar por alto, ya que podría afectar negativamente a sus actividades y a su negocio. Por este motivo, una plataforma de gestión de consentimiento líder como Usercentrics CMP puede marcar la diferencia al hablar de privacidad de datos.

Usercentrics ayuda a las empresas a cumplir con normativas esenciales como el RGPD y la CCPA, entre otras. Permite a las organizaciones recopilar, gestionar y documentar el consentimiento del usuario en sus sitios web y aplicaciones de forma eficiente y conforme a la normativa sin comprometer la experiencia del usuario.

Un CMP también disipa las preocupaciones de unos clientes cada vez más concienciados e informados sobre su privacidad, y les da el control sobre el acceso a sus datos. Usercentrics puede proporcionar soluciones que satisfacen las necesidades de todo tipo de empresas, ofreciendo privacidad a medida con más de 2.200 plantillas legales, análisis en profundidad y asistencia para ayudar a tu empresa a respetar la privacidad de los datos y cumplir con los requisitos de cumplimiento.

Mejor gestión del consentimiento y mayor confianza del consumidor

Usercentrics CMP automatiza el proceso de gestión del consentimiento para ayudarte a cumplir la normativa y respetar la privacidad de los clientes.

SABER MÁS

FAQS

¿Cómo afecta la privacidad de los datos a los equipos de marketing y ventas?

El éxito de los departamentos de marketing y ventas depende de la privacidad de los datos. Cumplir con la normativa de privacidad de datos, como obtener el consentimiento explícito del cliente, reduce el riesgo de incumplimiento y las sanciones económicas asociadas. También promueve la confianza del cliente y garantiza la recopilación ética de los datos necesarios de tu público objetivo a lo largo del funnel o embudo de ventas.

Esto implica un cambio de mentalidad en todos los equipos de marketing y ventas, asegurando que la privacidad de los datos sea una prioridad y se integre desde el inicio en todas las estrategias y campañas de marketing y ventas.

¿Cuál es un ejemplo de privacidad de los datos del consumidor?

Siempre que recopiles y proceses datos de consumidores, debes pedirles su consentimiento explícito cuando así lo exija la ley, asegurarte de que entienden por qué y cómo se procesan sus datos, y establecer medidas adecuadas para proteger sus datos.

Tu sitio web debe contar con una política de privacidad clara y actualizada que explique qué datos se recopilan, con qué fines, con quién pueden compartirse y cuáles son los derechos de los usuarios y cómo ejercerlos. El tratamiento de datos puede incluir el rastreo de cookies en el sitio web, la suscripción a newsletters, información sobre cuentas, etc.