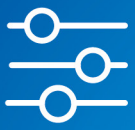
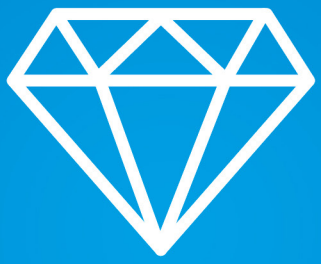
Principios Globales de Privacidad

SER CLARO Y TRANSPARENTE

RENDIR CUENTAS



RESPETAR LAS PREFERENCIAS DEL INDIVIDUO



VALORAR LA PRIVACIDAD

MANTENER SEGUROS A LOS DATOS PERSONALES

PROCESAR DATOS PERSONALES ÉTICAMENTE

ASUMIR RESPONSABILIDAD

GDMA

Global Data and Marketing Alliance

globaldma.com

GDMA
Global Data and Marketing Alliance

PREÁMBULO

Las nuevas tecnologías y el uso de los datos personales proveen a la humanidad la oportunidad de vivir mejor, consumir mejor y ser más sostenible. Los datos tienen un papel cada vez mayor en la búsqueda del crecimiento de las empresas, la innovación y la economía. Los beneficios derivables de los datos para la Sociedad y la economía solo pueden lograrse a través de su uso ético y la generación de confianza entre las personas y las organizaciones. Las reglas tanto de privacidad como de la protección de los datos contribuyen a la generación de confianza, a la vez de que facilitan un marco para el flujo libre y responsable de información en todo el mundo.

Los Principios Globales de la GDMA establecen un marco mundial para las Comunicaciones con clientes que deberían formar la base de todos los enfoques legales y comerciales. Están diseñados para ser un instrumento de mejores prácticas y su intención es servir como guía para la auto-regulación y para la legislación.

Estos Principios son compromisos aspiracionales para que las organizaciones, los gobiernos y las personas cultiven un ecosistema comercial transparente y exitoso que sirva a cada individuo con justicia, transparencia y respeto para su privacidad. El principio rector de respetar y valorar la privacidad engendra confianza en el corazón de las comunicaciones con clientes como un intercambio de valor entre una organización que busca prosperar y un individuo que desea beneficiarse. Los Principios aseguran que las organizaciones en todo el mundo pongan a la persona en el centro de todo lo que hacen, de modo que se pueda confiar en, respetar a y finalmente sostener a las organizaciones en todos los países.

GDMA
Global Data and Marketing Alliance

PRINCIPIOS

VALORAR LA PRIVACIDAD

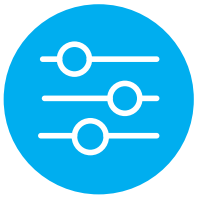
Respetar y valorar las expectativas de privacidad del individuo es crucial para generar confianza en todo el ecosistema de datos y marketing. Las organizaciones deben ayudar a los individuos a sentirse confiados y cómodos con respecto a las prácticas de marketing (por ejemplo – cuando navegan la web, reciban un email, utilicen una app en su móvil, o compren on- u offline) para generar beneficios tanto para el individuo, a través de la comunicación digna de confianza, como para la organización a través de la creación de valor mundial.

- Las organizaciones deben convertir a la "Privacidad" en un valor central a través de códigos o políticas que deben ser aprobados por la máxima dirección y comunicados a todos las partes interesadas.
- Las organizaciones deben tomar medidas para asegurar que sus empleados, socios y proveedores entiendan y se comprometan con los valores de la Privacidad.
- Las organizaciones deben capacitar y comprometer a sus empleados para que respeten y valoren la Privacidad y la seguridad de los datos.
- Las organizaciones deben adoptar un enfoque de privacidad desde el diseño.

SER CLARO Y TRANSPARENTE

Las organizaciones deben crear confianza, siendo claras y transparentes con los individuos con respecto a sus prácticas de recolección, uso y divulgación de sus datos personales.

Al recabar datos personales, las organizaciones deben facilitar (dentro de sus políticas de privacidad y más allá) información clara y de fácil acceso sobre:
- La identidad de la organización
- Qué datos personales se están recabando y cómo los van a utilizar.
- El propósito por el que se tratan los datos.
- Si planifican compartir los datos personales de los individuos, con qué tipo de organización y cómo.
- Los derechos del individuo de acceder a, rectificar, actualizar y suprimir sus datos personales, según las leyes aplicables localmente, y como el individuo puede ejercer estos derechos.



RESPETAR LAS PREFERENCIAS DEL INDIVIDUO

Las organizaciones deben respetar las preferencias del individuo con respecto al uso de sus datos personales para comunicaciones de marketing, siempre que sea legal y técnicamente posible hacerlo, como una manera de lograr una comunicación más eficiente en beneficio tanto del individuo como de la organización.

- Cada practicante de marketing debe facilitar al individuo una manera fácil para que exprese su preferencia con respecto a recibir comunicaciones de la organización.
- La organización también debe respetar las opciones de suprimir comunicaciones que imponen los gobiernos y las iniciativas de auto-regulación establecidas por la industria que les corresponden.
- Las organizaciones deben asegurar que los individuos tengan un claro entendimiento de las preferencias que han expresado y de cualquier procesamiento de datos que pudiera resultar de sus preferencias.

GDMA
Global Data and Marketing Alliance

PROCESAR DATOS PERSONALES ÉTICAMENTE

La correcta recolección, almacenamiento, uso y divulgación de los datos personales es esencial para mantener la integridad del ecosistema del marketing digital. Es necesario ejercer un cuidado especial cuando se realice el tratamiento de datos sensibles.

- Las organizaciones deben limitar la recolección de datos personales a los necesarios para cumplir con su propósito legítimo.
- Las organizaciones no deben utilizar o divulgar información personal para propósitos superfluos al motivo por el que ella fue recolectada.
- Las organizaciones deben almacenar información personal de manera segura y solamente para el período que sea necesario para cumplir con el propósito informado.
- Las organizaciones deben emplear especial diligencia cuando tratan datos personales que pudieran causar daño a los individuos si fueran mal administrados.
- Al recabar datos personales de niños, las organizaciones deben asegurar que toda la información requerida sea comprensible para el niño y sea facilitada por un padre o tutor legal.

ASUMIR RESPONSABILIDAD

Las organizaciones son responsables de los datos personales que utilizan para realizar actividades de marketing aun cuando sean transferidos o asignados a terceros (procesadores).

- Las organizaciones deben asegurar que todo empleado que esté involucrado en la gestión de datos personales y de marketing respete las prácticas de privacidad y protección de datos.
- Todo gerente de la organización es responsable de asegurar que los datos personales se utilicen responsablemente en todas las actividades bajo su área de influencia.
- Las organizaciones deben realizar regularmente capacitación interna sobre protección de datos para empleados implicados en el tratamiento de datos personales.
- Las organizaciones deben realizar regularmente auditorías de las practicas relacionadas con datos personales y deben mantener historiales de las mismas.
- Cuando se contrate a terceros para tratar datos, las organizaciones deben asegurar que sus actividades con respecto a datos personales y marketing respetan las prácticas de privacidad y protección de datos de la organización

GDMA
Global Data and Marketing Alliance

MANTENER SEGURO A LOS DATOS PERSONALES

Las organizaciones deben implementar las salvaguardas necesarias para proteger los datos personales de accesos, modificaciones, usos, divulgación o pérdidas no autorizadas.

• Las organizaciones deben implementar políticas escritas de seguridad y revisarlas periódicamente, además de realizar regularmente auditorías y pruebas de los sistemas tecnológicos que almacenan/administran/clasifican información personal.
• Las organizaciones deben restringir el acceso a sus sistemas en base a la "necesidad de conocer". Cada usuario debe tener acceso solamente a los datos personales que le sea requerido para cumplir con sus tareas.
• Siempre que sea posible, las organizaciones deben emplear la encriptación y/o seudonimización para salvaguardar los datos personales de los individuos, especialmente durante transferencia o almacenamiento en dispositivos móviles o portátiles.
• Las organizaciones deben aplicar un Enfoque Basado en los Riesgos al determinar qué medidas de seguridad implementar, asegurando que la información personal que pudiera causar daño tenga mayores niveles de seguridad y mayores limitaciones de acceso.
• Cuando sea apropiado, las organizaciones deberán notificar inmediatamente a las autoridades correspondientes, además de los sujetos afectados, sobre violaciones de la seguridad y deben asegurar que la información personal esté nuevamente asegurada y protegida después de una pérdida o acceso o divulgación no autorizado.

RENDIR CUENTAS

Las organizaciones deben demostrar que han adoptado e implementado los reglamentos internos necesarios, de acuerdo con estos Principios, para el uso responsable de los datos personales que tratan.

Para rendir cuentas, las organizaciones deben:
• Tener un programa que comprenda la administración de la privacidad.
• Tener una declaración clara y disponible al público que demuestre su compromiso con el cumplimiento de estos Principios.
• Mantener registros adecuados para demostrar su cumplimiento con estos Principios.
• Implementar un sistema adecuado de seguimiento y auditoria.
• Establecer programas internos para asegurar que los empleados deban rendir cuentas por su cumplimiento de la política establecida.
• Las organizaciones deben tener un programa vigente de administración de la privacidad y deben estar preparadas para demostrarlo, si corresponde, en particular frente al requerimiento de la agencia de protección de datos.

GDMA
Global Data and Marketing Alliance

DEFINICIONES

Datos personales: toda información sobre una persona física identificada o identificable («el individuo»).

Datos personales sensibles: datos personales que, si fueron divulgados sin consentimiento de su titular, podrían causar la marginalización del individuo y/o producirle un daño si personas no autorizadas tuvieran acceso a ellos. Por ejemplo: origen racial o étnico, orientación sexual, opiniones políticas, creencias o afiliaciones religiosas o filosóficas. Datos sobre menores también pueden ser sensibles.

Encriptación: Es el proceso de convertir información o datos en un código para prevenir accesos no autorizados. Frecuentemente se aplica a textos, mensajes, datos, documentos o imágenes, y para volver a la información ilegible a cualquier persona y/u organización que no tenga la clave de desencriptación.

Individuo: se refiere al sujeto, titular de los datos, que es una persona física que puede ser identificada, directa o indirectamente, a través de esfuerzos razonables y apropiados, especialmente por referencia a un identificador como un nombre, número de identificación, dato de localización, identificador online a uno o más factores particulares a la identidad física, fisiológica, genética, mental, económica cultural o social de dicha persona física.

Organización: se refiere a la persona legal/jurídica, compañía, asociación, fideicomiso, autoridad pública, agencia u otra entidad que, sola o en conjunto con otras, determina los propósitos y medios del tratamiento de datos personales. Las organizaciones pueden ser apoyadas por otras organizaciones que tratan datos personales de su parte (p.ej. servicios en la nube, contact centers, tercerización de procesos de negocios).

Política de privacidad / Aviso de privacidad: se trata de la explicación clara y detallada a los individuos de las prácticas que lleva a cabo la organización con respecto a los datos, cómo los recolecta, utiliza, almacena y comparte, así como también los derechos de los individuos de que sus datos sean protegidos, y la información sobre cómo proceder si un individuo cree que sus datos no han sido protegidos adecuadamente.

Privacidad desde el diseño: Este principio requiere que cualquier organización que diseñe un producto, servicio o proceso de datos o marketing piense de antemano sobre sus implicaciones en cuanto a la privacidad. Tener en cuenta las implicaciones para la privacidad al inicio e integrar las soluciones de privacidad en las primeras etapas de un proyecto, ayudará a la organización a identificar y atender cualquier problema potencial en su fase inicial.

Seudonimización: Se trata del tratamiento de datos personales de manera que se da un nombre a los datos que difiere de la identidad real del individuo de forma tal que los datos ya no puedan atribuirse a un individuo específico sin utilizar información adicional.

Tratamiento de datos personales: cualquier acción realizada sobre datos personales, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Violación de la seguridad de datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales.

GDMA

Global Data and Marketing Alliance

globaldma.com
info@globaldma.com

amdia