SINCH Mailjet

MANUAL

Kit de recursos RGPD

Guía para entender cómo afecta el RGPD
al mundo del marketing

Índice

Introducción

El Reglamento General de Protección de Datos de la Unión Europea, también conocido como RGPD, **entró en vigor en 2016, y se hizo de obligado cumplimiento el 25 de mayo de 2018**. A pesar de este periodo de adaptación previo, la obligación de su aplicación sorprendió a muchas empresas, que llegaron a ese mes de mayo sin estar completamente preparadas. Aún hoy, son muchas las que no lo tienen claro.

Según una encuesta realizada por Sinch Mailjet en 2021, tres años después de la aplicación de la ley aún eran muchos los profesionales del marketing que no tenían los conocimientos necesarios como para garantizar el cumplimiento de la normativa europea.

62,4 %

de los encuestados dijo que su empresa no "cumple plenamente" las normas de datos a las que están sometidos (RGPD, CCPA, CDPA...).

24,4 %

de los encuestados no sabe qué normas se les aplican en materia de protección de datos.

44,7 %

de las empresas encuestadas han tenido que suplementar o cambiar su tecnología de marketing para cumplir la normativa de datos pertinente.

La complejidad de algunos de sus requerimientos y procesos, así como la falta de concienciación, son algunas de las de las causas por las que muchas pymes aún no aplican con rigor los requisitos de esta normativa europea.

Esto supone un riesgo importante. **Las multas y sanciones por el no cumplimiento del RGPD son importantes**, así como lo es el daño reputacional que puede sufrir un negocio que no otorgue a los ciudadanos los derechos en materia de protección de datos que les corresponde. Por ello, lo más importante que debes recordar es que nadie está completamente exento. Independientemente del tamaño o la ubicación de la empresa, cualquier persona que recopile, procese y almacene datos personales de ciudadanos en la Unión Europea debe cumplir con él.

En Sinch Mailjet, la protección de datos personales siempre ha estado en el centro de nuestra filosofía de negocio y fuimos la primera compañía del mundo en obtener la certificación AFAQ de AFNOR Certification, que reconoce el cumplimiento de los principios del RGPD. Por eso, entendemos la complejidad que puede suponer para otras empresas el cumplimiento de la normativa y entendemos la importancia de educar a los profesionales del marketing en los principios del este reglamento europeo.

Este **Kit de recursos RGPD** reune todos los materiales que hemos ido creando a lo largo de los años para apoyar a los profesionales del marketing a adoptar los distintos cambios que se han ido produciendo en el campo de la protección de datos en España, Europa y el resto del mundo. ¿Nuestra misión? Ayudarte a ti y a tu empresa a cumplir con la normativa y a encontrar proveedores externos que también lo hagan.

No importa **si estás empezando desde cero o si estás comprobando** que no hayas pasado algo por alto. Estamos seguros de que esta información te será de **gran utilidad**.

> ***Importante:*** *Este documento y todos los materiales referenciados en él se suministran a título informativo únicamente. Si tienes dudas sobre la aplicación a tu negocio, te sugerimos que consultes con un abogado especialista para entender tus obligaciones exactas en relación con el RGPD.*

PARTE 1

Introducción al RGPD y a cómo te afecta

El principal problema con el que se encuentran muchas de las empresas que no saben si están aplicando correctamente el RGPD es su desconocimiento sobre la norma. Por eso, el primer paso es conocer la ley y sus ámbitos de aplicación.

¿Qué es el Reglamento General de Protección de Datos?

El Reglamento General de Protección de Datos de la Unión Europea (RGPD, o también conocido por sus siglas en inglés, GDPR) **entró en vigor en 2016 y es de obligado cumplimiento desde el 25 de mayo de 2018**. Este marco legislativo, que se ha convertido en un emblema de la protección de datos en todo el mundo, sustituyó a la pasada Directiva de Protección de Datos (95/46/EC).

Además, esta normativa europea contaba con la posibilidad de su desarrollo posterior a nivel nacional, como es usual para otras leyes de ámbito comunitario. En España esto se tradujo en **la Ley Orgánica 3/2018 de Protección de Datos y Garantía de los Derechos Digitales** (la LOPDGDD, o "la nueva LOPD"), que entró en vigor a finales de 2018.

¿A quién concierne el RGPD?

El RGPD se ha convertido en una norma de referencia a nivel mundial precisamente por su marco de aplicación, que ha obligado a empresas de todo el mundo a adaptarse a él.

Cualquier entidad u organización que trabaje con información personal de residentes europeos (ya sea B2B, B2C o ambas) debe cumplir con los requerimientos del RGPD, independientemente de dónde tenga su sede legal o sus diferentes centros de operaciones. En otras palabras, si una empresa recoge y trabajo con los datos de ciudadanos residentes en la Unión Europea, debe respetar el RGPD.

¿Cómo afecta el RGPD al mundo del marketing?

El Reglamento General de Protección de Datos afecta a cómo te comunicas e interactúas con tus clientes, y tiene un impacto directo en cómo tus clientes perciben tu marca. Con su entrada en vigor, cambiaron las normas de cómo se recopilaban, almacenaban y usaban los datos de los clientes, obligando a las empresas a auditar y cambiar sus procesos y proveedores.

Esencialmente, el RGPD y de la LOPDGDD establecen y refuerzan una serie de derechos para los individuos en cuanto a sus datos. Estos derechos son:

Consentimiento y permiso como piedras angulares del marketing

El control de los datos personales por parte de los clientes exige la implantación de políticas de transparencia en cuanto a la recolección de los datos por parte de las empresas, poniendo el consentimiento y la teoría del permiso en el centro de todas las actividades de marketing.

Las nuevas normas de protección de datos exigen que los usuarios den un **consentimiento informado y expreso al tratamiento y la recopilación de sus datos**. Esto afecta a técnicas tan habituales en el mundo del marketing como el opt in, el uso de casillas de verificación, la recopilación de los datos necesarios acordes con el uso que se establece... y también a los métodos para retirar dicho permiso por parte de los individuos cuando lo consideren oportuno.

¿Te parece excesivo? Pues lo cierto es que, aunque a priori estos requerimientos puedan parecer un problema a la hora de crear bases de datos de email o de ponerse en contacto con clientes y clientes potenciales, su cumplimiento es una práctica recomendable para una estrategia de marketing más efectiva.

Respetar el RGPD puede tener efectos beneficiosos para tus programas de comunicaciones de marketing, incluyendo el email, ya que se traduce en un mejor perfilado de los datos, unos usuarios más comprometidos y una base de datos más cuidada. Como hemos destacado muchas veces en nuestro blog, una mejor base de datos implica una mayor interacción, lo cual afecta positivamente a la entregabilidad de tus emails y al retorno de la inversión (ROI) de tus comunicaciones de marca.

Principales cambios introducidos por el RGPD

El Reglamento General de Protección de Datos introdujo cambios en los siguientes apartados:

1. **Definición de información personal:** El RGPD propuso una definición expandida de lo que se conoce como información personal para eliminar cualquier ambigüedad.
2. **Mayores derechos para los individuos:** La nueva normativa fortaleció los derechos de los individuos en lo relacionado a su información personal.
3. **Mayores responsabilidades para las empresas:** El RGPD también introdujo requerimientos más estrictos para quienes tratan y procesan información personal.
4. **Efecto extraterritorial:** El marco de aplicación de la ley se expandió más allá de nuestras fronteras para abarcar a cualquier empresa que tratara datos de ciudadanos europeos, sin importar su localización.
5. **Responsabilidad basada en el riesgo:** La ley exige a las empresas poner en marcha medidas técnicas y organizativas que prevengan cualquier tipo de riesgo sobre los datos personales almacenados.

6. **Requerimiento de notificar brechas de seguridad:** El RGPD obliga a las empresas a notificar a sus clientes de cualquier brecha de seguridad que haya podido afectar a sus datos personales.
7. **Introducción del Delegado de Protección de Datos:** Se introduce la figura del Delegado de Protección de Datos en empresas que cumplan ciertos requisitos.
8. **Privacidad por diseño:** Con el RGPD, la privacidad de datos se convierte en un requerimiento para las empresas que debe estar integrado en todos sus procesos técnicos y organizativos por diseño.

Puedes encontrar información más detallada de estos cambios aquí.

¿Cuáles son las multas por el no cumplimiento del RGPD?

La normativa europea estipuló también **sanciones por incumplimiento cuyos valores pueden ascender hasta los 20 millones de euros o el 4 % de los beneficios anuales** de una empresa, cualquiera que sea mayor de las dos. Esto significa que su incumplimiento ya no solo es cuestión de una posible pérdida de credibilidad o un daño a la reputación de una empresa, sino que tiene consecuencias financieras directas e importantes.

Riesgo económico

El RGPD estipula multas de hasta un 4% de los ingresos globales o 20 millones de euros, cualquiera que sea mayor.

Impacto en tu negocio

Las empresas no solo deben velar por su propio respeto a los requerimientos del RGPD, sino también asegurarse de contar con proveedores externos que garanticen su cumplimiento.

Retención de clientes

Aunque a corto plazo pueda parecer que las medidas del RGPD complican la actividad de la empresa, el incumplimiento puede suponer riesgos en la obtención y la retención de clientes.

Para profundizar

¿Quieres saber más sobre el RGPD y las normativas de protección de datos que afectan a España y otros países de Latinoamérica? Tenemos los recursos que necesitas:

- Respuestas a las principales preguntas sobre el RGPD
- Cuáles son los cambios clave con el RGPD
- Cómo puedo prepararme para el RGPD
- El RGPD y la nueva LOPD: La protección de datos en España en 2022
- Encuesta: ¿Se toman en serio las empresas las leyes de protección de datos?
- Protección de datos en Latinoamérica: Las leyes imprescindibles para el email marketing
- Auditoría de protección de datos en el email: RGPD, CAN-SPAM y CCPA

PARTE 2

El consentimiento en el mundo RGPD

En la sección anterior hemos hablado de la importancia del consentimiento y el permiso en el marco del Reglamento General de Protección de Datos.

Pero ¿qué es el consentimiento y cómo podemos asegurarnos de estar gestionándolo de forma correcta?

¿Cómo definimos el consentimiento en la era del RGPD?

Antes de la entrada en vigor del RGPD, se entendía por consentimiento "toda manifestación de voluntad libre, específica e informada por la que el interesado acepta el tratamiento de datos personales que le conciernen". Aunque era ya una definición bastante concreta, seguía dando pie a la ambigüedad, algo que el RGPD buscó corregir.

El Reglamento General de Protección de Datos de la Unión Europea define consentimiento como:

> *"Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".*

Esto significa que el consentimiento ahora debe ser intencionado y claro. No se considera válido como tal si se ha obtenido el consentimiento de una forma en la que no se pueda probar que el usuario/suscriptor era consciente del consentimiento que estaba otorgando y que ha tomado acciones para ello. Es decir, pone fin a las casillas premarcadas o a los consentimientos incluidos en la aceptación de términos y condiciones...

Esta nueva definición nos permite, podemos definir una serie de cualidades que debe cumplir el consentimiento explícito:

- **Descomprimido:** El consentimiento debe solicitarse de forma independiente a otras cuestiones como la aceptación de la Política de Privacidad, nunca de forma conjunta.
- **Activo:** El consentimiento debe otorgarse por medio de una acción clara. Seleccionar una casilla para marcarla, pinchar en un botón de "Aceptar" en una web, hacer clic en un email de confirmación de suscripción... Todas ellas son ejemplos de acciones que toma el suscriptor de forma voluntaria y afirmativa.
- **Granular:** Se debe requerir (y otorgar) el consentimiento de forma independiente para distintos fines y actividades. Por ejemplo, si queremos solicitar a un suscriptor que nos permita enviarle una newsletter semanal con ofertas y productos y otra newsletter mensual con un resumen de los puntos acumulados en su cuenta, debe hacerse por separado.

- **Nominal:** El consentimiento debe otorgarse a una empresa, organismo o individuo en particular y posibles terceros. Se recomiendan fórmulas como las que seguimos nosotros mismos en nuestra web: "Acepto que Mailjet se ponga en contacto conmigo...".
- **Documentado:** Debe mantenerse un registro del consentimiento. No sólo del hecho en sí, sino también de cuándo, cómo y a qué consintió cada suscriptor.
- **Fácil de retirar:** El proceso de retirar el consentimiento debe ser tan fácil como el de darlo. Debes dejar claro que el consentimiento que el suscriptor está otorgando puede retirarse en cualquier momento.
- **Sin desequilibrio en la relación:** Esta cualidad del consentimiento está enfocado a relaciones como las que puede tener una empresa con sus empleados. Dentro de los contratos debe existir un apartado en el que la empresa explicite cómo va a comunicarse con sus empleados y por qué canales. Puedes leer más sobre las características del consentimiento aquí.

¿Cómo solicitar el consentimiento acorde al RGPD?

Podría parecer que solicitar el consentimiento es ahora mucho más difícil, pero lo cierto es que existen muchas formas distintas para solicitarlo, tanto de forma virtual como presencial. Aquí compartimos algunos ejemplos:

- En la página web, **marcando una casilla**, junto a un texto que especifique para qué se solicita el consentimiento.
- En un email, **haciendo clic en un enlace** de opt in o de confirmación de consentimiento.
- En persona, **rellenando un formulario o declaración** de consentimiento.
- Por teléfono, **respondiendo "Sí"** a una solicitud clara de consentimiento verbal.
- En un apartado de configuración y ajustes de una aplicación, gestionando los distintos permisos y consentimientos que podemos encontrar en un panel de preferencias, por ejemplo.

Para ayudarte a preparar una solicitud de consentimiento, hemos preparado esta checklist con los distintos pasos que tienes que cubrir.

Checklist para la elaboración de una solicitud de consentimiento

- [ ] La declaración de consentimiento destaca y está separada de los Términos y Condiciones.
- [ ] La declaración de consentimiento pide a los usuarios que den su consentimiento en positivo.
- [ ] La declaración de consentimiento no usa casillas previamente marcadas o cualquier otro tipo de "consentimiento por defecto".
- [ ] La declaración de consentimiento usa un lenguaje claro, sencillo y fácil de entender.
- [ ] La declaración de consentimiento especifica por qué queremos los datos y qué vamos a hacer con ellos.
- [ ] La declaración de consentimiento está desgranada en opciones que cubren operaciones de procesamiento independientes.
- [ ] La declaración de consentimiento nombra de forma directa a nuestra organización y a proveedores externos que tendrán acceso a los datos.
- [ ] La declaración de consentimiento informa a los usuarios de que pueden retirar su consentimiento en cualquier momento.
- [ ] La declaración de consentimiento está formulada de tal forma que el usuario puede negarse a consentir sin detrimento alguno.
- [ ] La declaración de consentimiento no es una condición previa para un servicio.
- [ ] Si se ofrecen servicios online directamente a niños, la declaración de consentimiento solicita verificación de la edad e impone medidas para recabar el consentimiento paterno.

¿Cómo almacenar el consentimiento correctamente?

Igual de importante que la solicitud del consentimiento es mantener un registro correcto y adecuado de todos los consentimientos otorgados.

Con el RGPD debes asegurarte de almacenar:

- **Quién:** Nombre de la persona, nombre de usuario, ID de la sesión...
- **Cuándo:** Copia del documento fechado, registro en línea con fecha...
- **Qué se dijo:** Copia maestra del documento de consentimiento, con su versión y fecha, además de otras políticas de privacidad...
- **Cómo:** Por escrito (copia del documento), en línea (los datos enviados), oralmente (nota con el guión de la conversación)...
- **Si se ha retirado el consentimiento y cuándo se ha retirado.**

Para ayudarte en el almacenamiento y gestión del consentimiento, hemos preparado esta checklist con los distintos pasos que tienes que cubrir de forma regular.

Checklist para almacenar y gestionar el consentimiento

- [ ] Mi organización cuenta con un registro de almacenamiento del consentimiento que recoge quién, cuándo, cómo y a qué se otorgó el consentimiento.
- [ ] Mi organización ha puesto en práctica procesos para revisar los consentimientos con frecuencia y verificar que la relación, el procesamiento y la finalidad no han cambiado.
- [ ] Mi organización ha implementado procesos para actualizar el consentimiento a intervalos apropiados, incluidos los consentimientos paternos.
- [ ] Mi organización ha puesto en marcha mecanismos para facilitar la retirada del consentimiento en cualquier momento y comunica de forma clara cómo hacerlo, como por ejemplo la implementación de paneles de control de privacidad y otras herramientas de administración de preferencias.
- [ ] Mi organización actúa de forma rápida e inequívoca sobre las solicitudes de retirada del consentimiento.
- [ ] Mi organización no penaliza a aquellos que deseen retirar su consentimiento.

¿Por qué es importante cumplir con el RGPD en cuanto a consentimiento?

El RGPD es una normativa y, como tal, debemos cumplirla, o de lo contrario nos exponemos a cuantiosas multas y pérdida de confianza por parte de los clientes.

Pero, además, existen beneficios notables asociados con seguir estas mejores prácticas:

- Respeta el derecho de los clientes y suscriptores en cuanto al control sobre sus datos.
- Mejora las tasas de interacción al asegurarse de que únicamente las personas que tienen interés en tu marca reciben tus comunicaciones.
- Aumenta la confianza de los consumidores y mejora la reputación de tu marca.

Consejo profesional: Una forma más cómoda y segura de solicitar y registrar el consentimiento es mediante el uso del doble opt in, lo que te permite asegurarte al 100 % de que los usuarios han optado por darse de alta en tus comunicaciones.

Para profundizar

¿Quieres saber más sobre el consentimiento en el marco del RGPD? Échale un vistazo a estos recursos:

- Preguntas frecuentes sobre el consentimiento
- RGPD y el consentimiento
- Cómo gestionar tus contactos con Mailjet
- RGPD y la creación de perfiles
- Claves para enviar emails de forma segura
- RGPD: Pasos para demostrar el consentimiento de tus contactos con Mailjet

PARTE 3

Trabajar con proveedores externos en conformidad con el RGPD

Muchas empresas hoy en día dependen de proveedores externos para muchos de sus procesos internos y/o servicios, como el análisis de datos de marketing, el envío de emails, los CRM, la generación de clientes potenciales, el alojamiento web o los servicios de asistencia técnica.

Descubre cuáles son los requerimientos específicos para trabajar con proveedores externos en el marco del RGPD.

¿Por qué hablamos de proveedores externos en el contexto del RGPD?

Independientemente de quién procese los datos personales, de cara al RGPD tu empresa es responsable de la información personal que recoge y almacena de los clientes. Por tanto, si un proveedor externo incumple el RGPD, tú también lo estarás incumpliendo.

Esto puede no ser un problema si trabajas principalmente con proveedores que se encuentren dentro de la Unión Europea, ya que estarán muy familiarizados con la normativa, pero puede llegar a suponer un riesgo serio en el caso de los proveedores externos de otras partes del mundo como América, Asia u Oceanía.

En estos casos el RGPD es una normativa ajena a ellos, por lo que es importante asegurarse de que cumplen con ella.

Pasos a seguir a la hora de trabajar con proveedores externos

Hemos preparado una pequeña lista de cinco pasos a seguir para que tu empresa trabaje con sus proveedores de forma segura:

1. **Haz una lista de tus proveedores externos:** Necesitarás una lista tanto de las aplicaciones como de los proveedores de servicios externos que utilizas en cada departamento de tu empresa (sistema CRM, alojamiento en la nube, proveedores de email, herramientas de automatización...).
2. **Define el camino/ciclo que siguen tus datos:** Evalúa qué información se está compartiendo con los proveedores externos y cómo se procesan y/o almacenan esos datos.
3. **Revisa las medidas técnicas y organizativas:** Para cada proveedor y aplicación, identifica quién es la persona responsable de esos datos y cuáles son sus derechos de acceso, tanto externa como internamente, así como las medidas de protección de datos que existen.
4. **Evalúa el nivel de riesgo:** Identifica qué datos se ven afectados y, en base a tus averiguaciones anteriores, estima el nivel de riesgo de incumplimiento por parte de cada proveedor y aplicación.

5. En función de que cumplan o no con los requisitos, **verifica y examina los contratos** de la siguiente forma:
    - Si tus proveedores externos cumplen con el RGPD o estás razonablemente seguro de que van a hacer las modificaciones necesarias para empezar a cumplir con la normativa, haz que firmen nuevas cláusulas y que te aseguren que pueden proporcionarte pruebas de que cumplen con la normativa.
    - Si tus proveedores externos no cumplen con los requisitos, cámbialos o reemplázalos por otros que sí cumplan con el RGPD para evitar un posible daño a tu reputación y/o un riesgo financiero importante.

Sabemos que a veces es difícil saber qué preguntarles a los proveedores externos, incluidos los proveedores de servicios de email como Sinch Mailjet, para comprobar su cumplimiento. Por ello, hemos preparado esta lista de preguntas para que te asegures de que conoces todo lo que necesitas sobre tu proveedor actual.

Preguntas para comprobar el cumplimiento RGPD de proveedores externos

- [ ] ¿Qué categorías de datos personales procesan?
- [ ] ¿Procesan algún tipo de datos particularmente sensibles?
- [ ] ¿Qué tipo de procesamiento llevan a cabo?
- [ ] ¿Con qué propósito/s procesan los datos personales?
- [ ] ¿Durante cuánto tiempo procesan los datos personales?
- [ ] ¿Dónde almacenan sus datos y aplicaciones?
- [ ] ¿Alguna vez transfieren datos a centros de datos que se encuentran fuera de la UE?
- [ ] ¿Se me informa cada vez que transfieren mis datos?
- [ ] ¿Cuál es la base legal de la transferencia de datos?
- [ ] ¿Cuentan con un Delegado de Protección de Datos?
- [ ] ¿Qué controles de datos y procesos de gestión de riesgos han puesto en práctica?
- [ ] Para garantizar un nivel adecuado de protección de datos en su plataforma, ¿cómo gestionan el proceso de lanzamiento de la versión?
- [ ] ¿Quién tiene acceso a mis datos, en qué circunstancias y qué datos pueden consultarse? ¿Este acceso queda registrado?
- [ ] ¿Puedo realizar una auditoría de sus medidas técnicas y de seguridad sobre la protección de datos?
- [ ] ¿Cuentan con un proceso de notificación en caso de brecha de seguridad?
- [ ] ¿Tomaron medidas para cumplir a tiempo con el RGPD para mayo de 2018 y tienen en marcha políticas para mantener dicho cumplimiento?
- [ ] ¿Se pueden eliminar destinatarios de una lista de contactos específica? ¿Y de toda la base de datos?

- [ ] ¿Puede evitarse la retención de los datos enviados por una cuenta o limitarse dicha retención a un periodo específico de tiempo?
- [ ] ¿Pueden eliminarse las subcuentas de todas las bases de datos?
- [ ] ¿Pueden solicitar los usuarios que se recupere todos sus datos?
- [ ] ¿Puede alguien solicitar el acceso o la eliminación de datos para otra cuenta?
- [ ] ¿Podéis suministrarle a un destinatario una lista de todos los clientes que los tienen como destinatarios?
- [ ] ¿Puede un empleado solicitar que se eliminen todos sus datos?
- [ ] ¿Permiten que se transfiera la propiedad de una cuenta de un usuario a otro?
- [ ] ¿Tienen pruebas de que todos los contactos en una lista específica han sido añadidos con el consentimiento de los mismos?
- [ ] ¿Cómo protegen a los menores (como clientes o como destinatarios)?
- [ ] ¿Pueden suministrarle a un destinatario una lista de todos los clientes que los tienen como destinatarios?
- [ ] ¿Permiten que se elimine el enlace o el encabezado para darse de baja en sus plantillas para newsletters?
- [ ] ¿Pueden dar a los usuarios detalles sobre los datos que se monitorizan durante el uso de su web o aplicación?

Para profundizar

¿Quieres más información sobre cómo trabajar con proveedores externos en el marco del RGPD? Te dejamos algunos recursos útiles:

- Trabajar con un proveedor de soluciones de terceros de conformidad con el RGPD
- Cómo encontrar el proveedor de email perfecto
- El compromiso de Mailjet con la protección de datos

PARTE 4

ePrivacy: La regulación de las “cookies” tras el RGPD

Desde la entrada en vigor del RGPD, la Unión Europea ha seguido dando pasos adelante para reforzar la protección de datos de sus ciudadanos. Una de las normas con mayor impacto en las actividades de marketing de las empresas es la conocida como “Ley de cookies” o ePrivacy.

¿Qué es la normativa de ePrivacy y cuándo entra en vigor?

La ePrivacy, coloquialmente conocida como “Ley de cookies”, es una ley diseñada por la Comisión Europea para reforzar la protección de sus ciudadanos en cuanto a sus datos privados que restringe y modifica sustancialmente el uso de “cookies” y otras formas de rastreo y acumulación de información en línea.

En su origen, la normativa europea relativa a las “cookies” debía haber entrado en vigor y haberse implementado junto con el RGPD, pero su complejo desarrollo y proceso de aprobación ha dilatado en el tiempo su entrada en vigor.

Aunque aún no existe un texto final aprobado, parece que hay un consenso cercano y podría aprobarse en algún momento de este año 2024 o el año próximo. Eso significaría que, contando con un periodo de gracia similar al que tuvo el RGPD de dos años, sería de obligado cumplimiento en 2026 o 2027.

¿Cómo puede afectar ePrivacy a las empresas y cómo pueden estas prepararse para su entrada en vigor?

Hace unos años, al poco de la entrada en vigor del RGPD, Sinch Mailjet realizó una encuesta sobre los posibles efectos de la “Ley de cookies”. En ella, le pedimos a los profesionales de marketing que nos dieran su opinión sobre cómo creían que ePrivacy iba a afectar a sus departamentos y empresas. Los resultados fueron bastantes significativos ya entonces:

91 %

de los encuestados creía que las consecuencias de ePrivacy se traducirían en un descenso del tráfico a nivel global.

30 %

de los encuestados se planteaban reducir ya la cantidad de publicidad en función de cookies y de pago que llevaban a cabo.

79 %

de los profesionales de marketing predijo que incrementarían el uso del email marketing como canal de marketing digital tras la entrada en vigor de ePrivacy.

Muchos de los encuestados han llevado a cabo parte de esos cambios durante estos años y están ahora más preparados para afrontar la nueva normativa cuando por fin vea la luz. En cualquier caso, y para evitar sustos posteriores, es buena idea revisar las políticas de “cookies” y los métodos de recopilación de datos, ya que serán probablemente de los más afectados por ePrivacy.

La AEDP ya publicó una guía en 2019 sobre cómo tratar con las cookies, que luego actualizó en 2022 y en 2024, en la que se recogen ciertas cuestiones en las que parece existir cierto consenso, a pesar de que la norma aún no esté aprobada a nivel europeo.

Para profundizar

¿Quieres saber más sobre ePrivacy? Te dejamos algunos recursos útiles:

- Propuesta para la regulación ePrivacy
- Ley de Cookies RGPD: ¿Qué es el ePrivacy y cómo afectará a tu negocio?
- Encuesta sobre la percepción del ePrivacy post-RGPD (en inglés)

Conclusión

El Reglamento General de Protección de Datos de la Unión Europea es una normativa de obligado cumplimiento para todas aquellas organizaciones que trabajan con datos de la Unión Europea. Sin embargo, aún hay muchas empresas, sobre todo pymes, que no cumplen con la normativa o desconocen si lo hacen.

Y es que el RGPD no es solo una norma que afecte a los procesos internos de gestión de datos de las empresas, sino también a los proveedores externos que se utilizan en el día a día de los departamentos de marketing. Asegurarse de conocer y respetar los requerimientos del RGPD, así como de contratar los servicios de terceros que también los respeten, es clave para evitar multas sustanciales y posibles consecuencias reputacionales para tu empresa.

En Sinch Mailjet nos tomamos la protección de los datos personales muy en serio. Por eso, hemos desarrollado una plataforma que pone la seguridad de datos en el centro de nuestra actividad y trabajamos día a día por ofrecer toda la información y contenidos educativos necesarios para ayudar a nuestros clientes a cumplir con todas las normativas vinculantes a nivel global.

Descubre más sobre nuestro compromiso aquí.

Más de 40 000 empresas de todo el mundo utilizan Sinch Mailjet para reforzar las conexiones con sus clientes y suscriptores e impulsar su negocio a través del email marketing. Marcas como LaLiga, American Express, Microsoft o McDonalds confían en Mailjet para enviar miles de millones de emails cada año. Mailjet combina un editor de emails de arrastrar y soltar intuitivo con funciones de entregabilidad fáciles de usar que permiten a las empresas crear y enviar emails efectivos sin tocar una sola línea de código.

Fundada en París en 2010, Mailjet tiene oficinas por todo el mundo, incluyendo España, Francia, Reino Unido, Alemania y Estados Unidos. Mailjet se ha unido a Sinch, un proveedor líder de plataformas de comunicación como servicio (CPaaS) que ofrece soluciones de comunicación por mensajería, voz y vídeo a una extensa base de clientes a nivel mundial. Mailjet cuenta con la certificación ISO 27001 y cumple con el RGPD, por lo que ofrece a sus clientes los niveles más altos de seguridad y privacidad de datos.

Para más información, visita **mailjet.com/es**.