

The General Data Protection Regulation (GDPR)



What it is, what we are doing,
and what you can do



The GDPR sets a high bar for privacy rights and compliance for organizations, including Mailchimp and our customers. The goal of this guide is to help our customers understand their obligations under the GDPR and explain what steps we've taken to address GDPR compliance.

Please note that this guide is for informational purposes only, and should not be relied upon as legal advice. We encourage you to work with legal and other professional counsel to determine precisely how the GDPR might apply to your organization.

What is the GDPR?

We suspect you've heard of the GDPR. The General Data Protection Regulation (or "GDPR" for short) is a European privacy law that came into force on May 25, 2018 and was intended to strengthen, harmonize, and modernize EU data protection law and enhance individual rights and freedoms, consistent with the European understanding of privacy as a fundamental human right. The GDPR regulates how individuals and organizations may obtain, use, store, and share personal data. As a regulation, it must be followed in its entirety throughout the EU. In other words, it replaced the previous patch work of local member state data protection laws that were implemented under the old Data Protection Directive and put in place on regulation to bind all.

Does the GDPR apply to me?

The scope of the GDPR is very broad. It applies to (1) all organizations established in the EU, and (2) all organizations that target or monitor individuals in the EU. Essentially, this means the GDPR will apply to most organizations that process personal data of EU individuals—regardless of where they are established, and regardless of where their processing activities take place. This means the GDPR could apply to any organization anywhere in the world, across all industries and sectors. You should perform your own analysis to determine to what extent (if any) your organization may be subject to the GDPR.

Key Concepts

There are a few definitions that will aid the understanding of the GDPR's broad scope.

What is considered "personal data"? Personal data is any information relating to an identified or identifiable individual; meaning information that could be used, on its own or in conjunction with other data, to identify an individual. Consider the extremely broad reach of that definition—it includes not only information that's commonly considered to be personal in nature (e.g., social security numbers, names, physical addresses, email addresses), but also data such as IP addresses, behavioral data, location data, biometric data, financial information, and much more. This means that, for Mailchimp customers, at least a majority of the information that you collect about your contacts will be considered personal data under the GDPR.

The broad definition encompasses work email addresses containing an individual's name or any business contact information tied to or related to an individual, such as the individual's name, job title, company, business address, work phone number, etc. In contrast, personal data doesn't include



generic business names, business addresses, generic email addresses or any other general business information, as long as this information hasn't been linked to an individual. So, for example, "John.Smith@mailchimp.com" would most likely be considered "personal data" governed by the GDPR whereas "contact@mailchimp.com" wouldn't.

It's also important to note that even information that cannot identify a particular individual on its own but which could be combined with other information to identify an individual (known as "pseudonymous data") is considered personal data. So, for example, a hashed email address will still be considered personal data, albeit pseudonymized.

Sensitive personal data, such as health information or information that reveals a person's racial or ethnic origin, requires even great protection. You must not store data of this nature within your Mailchimp account.

What does it mean to "process" data? Processing is any operation which is performed on personal data, whether or not by automated means. This includes collecting, recording, organizing, structuring, storing, adapting, retrieving, using, combining, erasing, destroying, disclosing, disseminating, or otherwise making available personal data.

Basically, if you're collecting and managing any personal data of individuals physical residing in Europe (even if they're not citizens), you're processing personal data within the meaning prescribed by the GDPR. This means, for example, that if any of your Mailchimp audiences contain the email address, name, or other personal data of an individual located in Europe, then you're processing personal data under the GDPR.

What's the difference between a data controller and a data processor? If you process personal data, you do so either as a controller or a processor, and there are different requirements and obligations that will apply to you depending on which role you perform. It's important to understand whether you are acting as a controller or a processor and to familiarize yourself with the responsibilities that apply to you.

A controller is the organization that determines the purposes and means of processing — they make the important decisions like what personal data is collected, what the data is used for, how long it's retained and who it's shared with. A processor is an organization that merely processes the data on behalf of the controller and follows the controller's instructions. This typically means a processor can't use personal data for any other purpose than to provide a service to the relevant controller.

Controllers retain primary responsibility for compliance with the GDPR (including, for example, the obligation to give notice to individuals about processing, respond to individuals exercising their privacy rights, and report security breaches to data protection authorities); however, the GDPR also places some direct responsibilities on processors.

In the context of Mailchimp, in the majority of circumstances our customer acts as the controller. Our customers, for example, decide what information from their contacts is uploaded or transferred into their Mailchimp account; direct Mailchimp, through our application, to send emails to certain contacts on their email distribution lists; and instruct Mailchimp to place advertisements on their behalf on third party platforms such as Facebook or Instagram.



Mailchimp acts as a processor by performing these and other services for our customers.

There are certain cases where we act as a controller, such as where we process customer information for our own business purposes (like account management and billing) and for our data analytics project. You can find more information about our data analytics projects, including how you can opt out from data analytics, [here](#).

What are the key principles under the GDPR? The GDPR contains a number of key principles that must be followed when processing personal data to ensure compliance. It's a controller's responsibility to ensure compliance with these key principles.

- *Personal data must be processed in a fair, legal, and transparent way:* Individuals should be informed about how their personal data will be used and you should never use data in any way that the individual would not reasonably expect. You must also have a legal basis for processing personal data, such as with the individual's consent or based on your legitimate interests.
- *Personal data must be collected for specific, explicit, and legitimate purposes:* You should only collect personal data to fulfill specific purposes and not use data in a way that is incompatible with those purposes.
- *Personal data should be relevant and limited to what is necessary:* You should only collect the information you need and not collect or use unnecessary or redundant data.
- *Personal data should be accurate and kept up to date:* You should ensure that the data you hold is accurate and take steps to review and update information when necessary.
- *Personal data should only be kept for as long as necessary:* You should only store personal data for as long as you need it and shouldn't keep personal data indefinitely or "just in case".
- *Personal data must be kept safe and secure:* You must implement technical and organizational measures to protect personal data according to the type of data you process and the resources and technology available.

Most importantly, you must be able to demonstrate how you comply with these principles and show how you're accountable.

What rights do individuals have under the GDPR? The GDPR gives individuals a number of rights in relation to their personal data. You must ensure that you can accommodate these rights if you're processing personal data of EU individuals.

- *Right of access:* Individuals have the right to be given certain information about how their data has been collected and used and to obtain a copy of their data from you.
- *Right to rectification:* Individuals can request that their data be corrected or updated at any time.
- *Right of erasure (the "right to be forgotten"):* In certain circumstances, individuals can request that their data be deleted entirely.
- *Right to withdraw consent:* If you have obtained an individual's consent to process their personal data, they can withdraw their consent at any time.
- *Right to object:* Alternatively, if you rely on your legitimate interests to process an individual's data, the individual can object to your processing and you must stop doing so unless you can demonstrate that your interests override the interests and rights of the individual.



- *Right to object to marketing:* Individuals have an absolute right to object at any time to processing of their personal data for marketing purposes.
- *Right of portability:* Individuals can request that you transfer their data to another organization.

Organizations must respond to these requests within 1 month or, in exceptional cases, within 3 months. Except the right to object to marketing (which is absolute and must therefore always be complied with), certain exemptions to the above rights may apply. All requests should therefore be carefully reviewed.

How does the GDPR apply to email marketing? When it comes to email marketing regulation in Europe, the GDPR is only half the story. Europe also has a separate law - the Privacy and Electronic Communications Directive (or e-Privacy Directive) that contains supplemental rules governing consent requirements for e-marketing—i.e., marketing sent over electronic communication channels (such as phone, fax, e-mail and SMS). When sending e-marketing, these supplemental consent rules apply in addition to the need for businesses to identify lawful processing grounds under the GDPR.

Put simply, these rules require opt-in consent for e-mail and SMS marketing, unless an individual's contact details were collected in the context of a sale and the individual was given the ability to opt-out at that time. If so, first party e-mail and SMS marketing is possible on an opt-out basis (though third party e-mail and SMS marketing still require opt-in).

As the e-Privacy Directive is a Directive, meaning it has to be implemented into each member state's local law, you should check local member state law to double check the local requirements. For example, some countries (like the UK) are more relaxed about B2B email marketing (which can be done on an opt-out basis), while other countries (like Germany) have a stricter double opt-in requirement (see more on this below).

However, the GDPR is still relevant because most email addresses will be considered personal data and therefore subject to the GDPR's requirements. In particular, where you're required to obtain an individual's consent you must do so in accordance with the GDPR.

What does the GDPR say about consent? We're glad you asked. Consent isn't always required to process an individual's personal data. However, where you're required to obtain the individual's consent (which may apply if you're carrying out certain email marketing) you must ensure that you obtain consent in accordance with the GDPR's strict requirements:

- *Consent must be opt-in:* Individuals must explicitly opt-in to the collection and use of their personal data. This means that silence, pre-checked boxes, and implied opt-ins (i.e., inactivity) aren't valid.
- *Consent must be informed:* This means you must provide meaningful information to individuals about why you're collecting the information and clearly explain how you plan to use it. This information should be provided at the time individuals give their consent.
- *Consent must be specific:* This means separate consent should be obtained for different processing activities and you shouldn't try to bundle different purposes within 1 consent.



- *Consent must be freely-given:* This means individuals must have a genuine choice when consenting and their consent should not be conditional on receiving a product or service.
- *Consent must be demonstrable:* Don't forget you must be able to demonstrate that you've obtained consent, including who consented, when, and what information was given to the individual at the time.

Lastly, keep in mind that certain countries (like Germany) require "double opt-in" consent to carry out email marketing. Double opt-in involves an extra confirmation step that verifies each email address. Although this is not required by the GDPR, or by every EU member state, we recommend you enable double opt-in when sending electronic marketing communications to EU individuals as this represents the gold standard for GDPR compliance.

Does the GDPR say anything about cross-border data transfers? Yes, the GDPR contains provisions that address the transfer of personal data from EU member states to third-party countries, such as the United States. The GDPR doesn't contain any specific requirement that the personal data of EU individuals be stored only in EU member states. Rather, the GDPR requires that certain conditions be met before personal data is transferred outside the EU, identifying a number of different mechanisms that organizations can use to perform cross-border data transfers: adequacy decisions, standard contractual clauses, binding corporate rules, certification mechanisms, and codes of conduct. The primary purpose of these mechanisms is to ensure that when the personal data of Europeans is transferred abroad, the protection travels with the data.

An adequacy decision is a decision by the European Commission that the country or territory where the personal data is being transferred provides an adequate level of protection. Prior to the 2020 decision invalidating the EU-US and Swiss-US Privacy Shield Frameworks, the EU-US Privacy Shield framework was one such example of an adequacy decision. Mailchimp will continue to protect EEA, UK, and Swiss data in compliance with the Privacy Shield Principles to which it has certified compliance.

In addition, Mailchimp contractually commits to transfer and process all of its users' Swiss, EU, and UK data in compliance with the EU's Standard Contractual Clauses, which remain a valid data export mechanism and which automatically apply in accordance with Mailchimp's Data Processing Addendum.

If you are transferring personal data to other organizations that are located outside the EU, then you should ensure you have an appropriate ground to perform the cross-border data transfer, such as an adequacy decision or Standard Contractual Clauses approved by the European Commission.

Does the GDPR still apply to the UK after Brexit? The EU GDPR is an EU Regulation and it no longer applies to the UK. However, any business that operates inside the UK, must comply with UK data protection law. The GDPR has been incorporated into UK data protection law as the UK GDPR – so in practice there is little change to the core data protection principles, rights and obligations found the UK GDPR.



Also, remember that if you're based in the UK but target or monitor EU individuals you'll still be subject to the GDPR even after the end of the transition period.

What happens if you don't comply with the GDPR? Non-compliance with the GDPR can result in large financial penalties. Sanctions for non-compliance can be as high as 20 million Euros or 4% of global annual turnover, whichever is higher.

How does Mailchimp comply with the GDPR? At Mailchimp, we believe that the GDPR is an important milestone in data privacy and support its high standards. For a full explanation of how we comply with the GDPR, please see our [FAQs](#). To summarize, we've addressed GDPR compliance by:

- Ensuring our privacy policies clearly explain Mailchimp's commitment to the GDPR, are transparent about how we use personal data and give individuals information about how they can exercise their data privacy rights.
- Incorporating the EU's Standard Contractual Clauses in our [Data Processing Addendum](#) which automatically forms part of our Standard Terms of Use (our contract with you) and applies to customer data protected by EU laws.
- Providing our customers with GDPR-ready terms in our Data Processing Addendum and updating our contracts with third party vendors to ensure they're GDPR-compliant.
- Building new GDPR-friendly features and templates to add to our application.
- Appointing a Data Protection Officer (DPO) to oversee our compliance program.
- Certifying annually with the EU-U.S./Swiss-U.S. Privacy Shield Frameworks and continuing to protect EEA, UK, and Swiss data in compliance with the Privacy Shield Principles.

We also complete a SOC II Type 2 examination on an annual basis for the Trust Principal Criteria of Security, Processing Integrity, Confidentiality, and Availability.

How can Mailchimp assist me in meeting GDPR requirements? There are several ways in which Mailchimp can help you with your GDPR compliance.

Tools and features: We offer a number of tools and features that help our customers meet their obligations under the GDPR.

- GDPR-friendly forms that include checkboxes for opt-in consent by default, and editable sections that allow you to explain how and why you're using contact data. To learn more about using GDPR-friendly forms, check out [Collect Consent with GDPR Forms](#).
- Various opt-in settings, including the option for double opt-in. You can find out how to choose opt in-settings [here](#).
- Tools to export and delete contact information, which can help you to prove consent and fulfill deletion and access requests. You can learn more about these tools [here](#) and [here](#).
- Additional fields within the Mailchimp API for marketing permissions, so you can enable GDPR fields and sync contact marketing permissions across your audiences.
- To learn more about managing your audience with the Mailchimp API, check out our [API documentation](#).



- Additional security features to help you prevent unauthorized access to your account and give you greater control over your data. You can learn more about these features [here](#).

Individuals' rights: Mailchimp can help you promptly respond to requests from your contacts pursuant to their individual rights under the GDPR.

- *Right of access:* You can export data about individual contacts from your Mailchimp account, which can help you fulfill access requests. You can learn how to do this [here](#).
- *Right to be forgotten:* You can delete contacts from your Mailchimp account at any time. You can learn how to do this [here](#). It's important to remember that Mailchimp audiences work independently of each other and deleting a contact from one audience doesn't ensure that the same email address will also be deleted from other audiences in your account. You can learn how to search for a contact across all audiences [here](#).
- *Right to object:* As explained above, if a contact objects to you processing their personal data you can remove them from your Mailchimp account at any time.
- *Right to rectification:* You can access and update your contacts' profiles within your Mailchimp account to correct or complete their contact information at any time. You can learn how to do this [here](#).
- *Right of portability:* As explained above, you can export data about individual contacts from your Mailchimp account at any time. The export folder will include CSV files that display all contact data stored in your account for the individual.

Providing individuals with notice and obtaining consent: You must lawfully obtain and process email addresses and other personal data from your contacts.

- The personal data of your contacts may be collected and transferred to Mailchimp via pop-up and embedded forms made available in our application and designed by you. These forms are one of the most important Mailchimp tools you can use as it relates to your GDPR compliance. Even better, they are easy to use and you can design them to meet your specific GDPR compliance needs.
- You should carefully design each of these forms to make sure that language in the body and/or footer is clear, specific, and covers all possible reasons for using the information being solicited. Be very specific about the intended use of the information you're collecting.
- Where required, it's your responsibility to ensure that you obtain consent from your customers and contacts to send their information to Mailchimp for processing, so you should ensure that all of your pop-up windows, forms, etc. include language that provides this consent.
- We suggest selecting double opt-in for audience sign-ups.
 - Note that this may not be the default setting if you don't enable our GDPR-friendly sign up forms.
- The ability of your contacts to withdraw consent or change preferences should be easily accessible. Mailchimp's "unsubscribe" and "preferences" footer options can help.
 - An "[unsubscribe](#)" option is automatically included in the footer of every campaign sent through Mailchimp. This allows any campaign recipient to easily unsubscribe from your Mailchimp audience, thereby helping you comply with your GDPR obligations when a subscriber withdraws his or her consent to receive marketing emails.



- You also have the option to include a “[preferences](#)” link in the footer of any campaign, which will give any recipient the ability to easily update their profile details within your Mailchimp account, helping you meet the GDPR’s right to rectification requirement.
- Make sure that you are frequently updating any information stored within your Mailchimp account that relates to your contacts, such as name and contact information, when requested to do so by a subscriber or contact.
- You should also ensure that you’re keeping accurate records, especially of your contacts’ consent permitting you to send them marketing emails, store and use their personal data, and any other processing activities you’re undertaking. Mailchimp can help you obtain consent and will store a record of your contacts’ consent in your Mailchimp account. When you use a Mailchimp signup form to add contacts to your account, Mailchimp records the email address, IP address, and timestamp associated with every subscriber or contact who completes and submits the form.
- Keep in mind that any consent you obtain from your contacts must comply with the GDPR and e-Privacy requirements, irrespective of when that consent was obtained.
- You should review any Mailchimp integrations or add-ons that you’re using (or plan to use), and any terms associated with those, to ensure that you’ve adequately disclosed potential data processing activities associated with your use of those services to your contacts. For example:
 - If you choose to use product retargeting emails or third-party remarketing ad features, or if you’ve connected your e-commerce store to your Mailchimp account, your website may set a Mailchimp cookie which allows for tracking certain activities of your contacts. Other pixels may also be set on your website through this cookie and those will be described in the specific terms applicable to each feature. You should ensure that you implement an appropriate cookie notice and consent mechanism with respect to your use of cookies and related pixels.
- You should review the privacy statement and practices applicable to your organization and ensure that they provide proper notice that the personal data of your contacts will be transferred to and processed by Mailchimp. Mailchimp’s Standard Terms require that you clearly post, maintain, and abide by a publicly accessible privacy notice that (a) satisfies the requirements of applicable data protection laws, (b) describes your use of the Service, and (c) includes a link to Mailchimp’s Privacy Policy. You may also want to specifically identify the applicable processing activities performed by Mailchimp, such as the collection (e.g., via sign-up forms) and storage of personal data (e.g., within your Mailchimp account in order to allow you to create and use distribution lists, send marketing email campaigns, and place online advertisements), and the transfer of personal data to certain Mailchimp sub-processors (who, as described in our Data Processing Agreement, perform some critical services, such as helping Mailchimp prevent abuse and providing support to our customers).

If you have any specific questions about the information above, or additional questions related to your use of Mailchimp, you can email dpo@mailchimp.com.

Last Updated: April 2020