mailchimp

The General Data Protection Regulation (GDPR)

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

The GDPR will become enforceable on May 25, 2018, and will set a high bar for global privacy rights and compliance. We are actively preparing our business and compliance processes for the GDPR to take effect, and this guide is intended to help our customers do the same.

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?
By now, you have likely heard of the GDPR: the General Data Protection Regulation, a European privacy law approved by the European Commission in 2016. The GDPR will replace a prior European Union privacy directive known as Directive 95/46/EC (the "Directive"), which has been the basis of European data protection law since 1995.

A regulation such as the GDPR is a binding act, which must be followed in its entirety throughout the EU. The GDPR is an attempt 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, among other things, how individuals and organizations may obtain, use, store, and eliminate personal data. It will have a significant impact on businesses around the world.

When does it come into effect?
The GDPR was adopted in April 2016, but will officially be enforceable beginning on May 25, 2018. There will not be a "grace period," so it is important that organizations impacted by the GDPR get ready for it now.

Who does it affect?
The scope of the GDPR is very broad. The GDPR will affect (1) all organizations established in the EU, and (2) all organizations involved in processing personal data of EU citizens. The latter is the GDPR's introduction of the principle of "extraterritoriality"; meaning, the GDPR will apply to *any organization processing personal data of EU citizens*—regardless of where it is established, and regardless of where its processing activities take place. This means the GDPR could apply to any organization anywhere in the world, and all organizations should perform an analysis to determine whether or not they are processing the personal data of EU citizens. The GDPR also applies across all industries and sectors.

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

What is considered "personal data"? Per the GDPR, 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. Personal data will now include not only data that is 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 users, at least a majority of the information that you collect about your subscribers and contacts will be considered personal data under the GDPR. It's also important to note that even personal data that has been "pseudonymized" can be considered personal data if the pseudonym can be linked to any particular individual.

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

What does it mean to "process" data? Per the GDPR, processing is "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." Basically, if you are collecting, managing, using or storing any personal data of EU citizens, you are processing EU personal data within the meaning prescribed by the GDPR. This means, for example, that if any of your Mailchimp lists contains the email address, name, or other personal data of any EU citizen, then you are processing EU personal data under the GDPR.

Keep in mind that even if you do not believe your business will be affected by the GDPR, the GDPR and its underlying principles may still be important to you. European law tends to set the trend for international privacy regulation, and increased privacy awareness now may give you a competitive advantage later.

How is the GDPR different from the Directive? How are obligations changing?
While the GDPR preserves many principles established by the Directive, it introduces several important and ambitious changes. Here are a few that we believe are particularly relevant to Mailchimp and our customers:

1. Expansion of scope: As mentioned above, the GDPR applies to all organizations established in the EU or processing data of EU citizens, thus introducing the concept of extraterritoriality, and broadening the scope of EU data protection law well beyond the borders of just the EU.
2. Expansion of definitions of personal and sensitive data, as described above.
3. Expansion of individual rights: EU citizens will have several important new rights under the GDPR, including the right to be forgotten, the right to object, the right to rectification, the right of access, and the right of portability. You must ensure that you can accommodate these rights if you are processing the personal data of EU citizens.
    - *Right to be forgotten:* An individual may request that an organization delete all data on that individual without undue delay.
    - *Right to object:* An individual may prohibit certain data uses.

- *Right to rectification:* Individuals may request that incomplete data be completed or that incorrect data be corrected.
- *Right of access:* Individuals have the right to know what data about them is being processed and how.
- *Right of portability:* Individuals may request that personal data held by one organization be transported to another.

4. Stricter consent requirements: Consent is one of the fundamental aspects of the GDPR, and organizations must ensure that consent is obtained in accordance with the GDPR's strict new requirements. You will need to obtain consent from your subscribers and contacts for every usage of their personal data, unless you can rely on a separate legal basis, such as those found in number 5 below. The surest route to compliance is to obtain explicit consent. Keep in mind that:
   - Consent must be specific to distinct purposes.
   - Silence, pre-ticked boxes or inactivity does not constitute consent; data subjects must explicitly opt-in to the storage, use and management of their personal data.
   - Separate consent must be obtained for different processing activities, which means you must be clear about how the data will be used when you obtain consent.
5. Stricter processing requirements: Individuals have the right to receive "fair and transparent" information about the processing of their personal data, including:
   - Contact details for the data controller, which we will explain in more detail below.
   - Purpose of the data: This should be as specific ("purpose limitation") and minimized ("data minimization") as possible. You should carefully consider what data you are collecting and why, and be able to validate that to a regulator.
   - Retention period: This should be as short as possible ("storage limitation").
   - Legal basis: You cannot process personal data just because you want to. You must have a "legal basis" for doing so, such as where the processing is necessary to the performance of a contract, an individual has consented (see consent requirements above), or the processing is in the organization's "legitimate interest."

There are many other principles and requirements introduced by the GDPR, so it is important to review the GDPR in its entirety to ensure that you have a full understanding of its requirements and how they may apply to you.

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's provisions regarding cross-border data transfers, however, do not radically differ from the provisions in place under the Directive. The GDPR, like the Directive, does not contain any specific requirement that the personal data of EU citizens 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 legal grounds that organizations can rely on to perform cross-border data transfers.

One legal ground for transferring personal data set out in the GDPR is an "adequacy decision." An adequacy decision is a decision by the European Commission that an adequate level of

protection exists for the personal data in the country, territory, or organization where it is being transferred. The Privacy Shield framework constitutes one such example of an adequacy decision. Mailchimp participates in and has certified its compliance to the Privacy Shield framework, and we are committed to treating all personal data received from EU member countries in accordance with the Privacy Shield framework's applicable principles.

What does this mean for you? Generally speaking, it means we expect that Mailchimp's EU customers will be able to continue to rely on Mailchimp's Privacy Shield certification in order to transfer their lawfully obtained personal data to Mailchimp under the GDPR.

Do you need to comply with the GDPR?
You should consult with legal and other professional counsel regarding the full scope of your compliance obligations. Generally speaking, however, *if you are an organization that is organized in the EU or one that is processing the personal data of EU citizens, the GDPR will apply to you*. Even if all that you are doing is collecting or storing email addresses, if those email addresses belong to EU citizens, the GDPR likely applies to you.

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

Does it matter whether you are a controller or a processor?
If you access personal data, you do so as either a controller or a processor, and there are different requirements and obligations depending on which category you are in. A controller is the organization that determines the purposes and means of processing personal data. A controller also determines the specific personal data that is collected from a data subject for processing. A processor is the organization that processes the data on behalf of the controller.

The GDPR has not changed the fundamental definitions of controller and processor, but it has expanded the responsibilities of each party.

Controllers will retain primary responsibility for data protection (including, for example, the obligation to report data breaches to data protection authorities); however, the GDPR does place some direct responsibilities on the processor, as well. Accordingly, it is important to understand whether you are acting as a controller or a processor, and to familiarize yourself with your responsibilities accordingly.

In the context of the Mailchimp application and our related services, in the majority of circumstances, our customers are acting as the controller. Our customers, for example, decide what information from their contacts or subscribers is uploaded or transferred into their Mailchimp account; direct Mailchimp, through our application, to send emails to certain

subscribers on their email distribution lists; and instruct Mailchimp to place advertisements on their behalf on third party platforms such as Facebook or Instagram. Mailchimp is acting as a processor by performing these and other services for our customers.

Will Mailchimp comply with the GDPR?
Mailchimp is excited about the GDPR and the strong data privacy and security principles that it emphasizes, many of which Mailchimp instituted long before the GDPR was enacted. At Mailchimp, we believe that the GDPR is an important milestone in the data privacy landscape, and we are committed to achieving compliance with the GDPR on or before May 25, 2018.

Mailchimp's GDPR preparation started more than a year ago, and as part of this process we are reviewing (and updating where necessary) all of our internal processes, procedures, data systems, and documentation to ensure that we are ready when the GDPR goes into effect. While much of our preparation is happening behind the scenes, we are also working on a number of initiatives that will be visible to our users. We are, among other things:

- Updating our Data Processing Agreement to meet the requirements of the GDPR in order to permit you to continue to lawfully transfer EU personal data to Mailchimp and permit Mailchimp to continue to lawfully receive and process that data;
- Updating our third-party vendor contracts to meet the requirements of the GDPR in order to permit us to continue to lawfully transfer EU personal data to those third parties and permit those third parties to continue to lawfully receive and process that data;
- Analyzing all of our current features and templates to determine whether any improvements or additions can be made to make them more efficient for those users subject to the GDPR;
- Evaluating potential new GDPR-friendly features and templates to add to our application.

Mailchimp has self-certified to both the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield regimes, and lawfully transfers EU/EEA personal data to the U.S. pursuant to our Privacy Shield Certification. 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.

In addition, we will be prepared to address any requests made by our customers related to their expanded individual rights under the GDPR:

- *Right to be forgotten:* You may terminate your Mailchimp account at any time, in which case we will permanently delete your account and all data associated with it.
- *Right to object:* You may opt out of inclusion of your data in our data science projects simply by changing the Privacy Setting on your account. This process is explained in the following article, under the "Data Science and Privacy" sub-heading: http://kb.mailchimp.com/accounts/login/set-account-security-options.
- *Right to rectification*: You may access and update your Mailchimp account settings at any time to correct or complete your account information. You may also contact Mailchimp at any time to access, correct, amend or delete information that we hold about you, as explained in Section 19 of our Privacy Policy.

- *Right of access*: Our Privacy Policy describes what data we collect and how we use it. If you have specific questions about particular data, you can contact privacy@mailchimp.com for further information at any time.
- *Right of portability*: We will export your account data to a third party at any time upon your request.

How can Mailchimp assist in your GDPR compliance efforts?
You should start your compliance efforts now, if you haven't already. It is never too early to review your organization's data privacy and security practices, and there are several ways in which Mailchimp can help.

Expansion of Individual Rights: Mailchimp can help you promptly respond to requests from your subscribers or contacts pursuant to their expanded individual rights under the GDPR.

- *Right to be forgotten*: You may delete individual subscribers upon their request at any time. More about deleting lists can be found here. In addition, as described below, individual subscribers may contact Mailchimp directly to request deletion of their data from individual Mailchimp user's accounts or across multiple Mailchimp users' accounts (to the extent the subscriber is on more than one Mailchimp users' list). It is important to remember that Mailchimp lists work independently of each other, and deleting a subscriber from one list does not ensure that same email address will also be deleted from other lists where it may be present.
- *Right to object*: You may opt out of inclusion of your subscribers' or contacts' data in our data science projects simply by changing the Privacy Setting on your account. This process is explained in the following article, under the "Data Science and Privacy" sub-heading: http://kb.mailchimp.com/accounts/login/set-account-security-options.
- *Right to rectification*: You may access and update your subscriber/contact lists within your Mailchimp account to correct or complete subscriber/contact information upon their request at any time. In addition, any data subject (including your subscribers and contacts) may contact Mailchimp directly to access, correct, and/or delete information that Mailchimp may hold about the data subject. As explained in Section 19 of our Privacy Policy: "Individuals may request to access, correct, amend or delete information we hold about them by contacting us here. Unless it is prohibited by law, we will remove any Personal Information about an individual, either you (our user) or a Subscriber, from our servers at your or their request. There is no charge for an individual to access or update their Personal Information."
- *Right of access*: Our Privacy Policy describes what data we collect and how we use it. As mentioned above, any of your subscribers or contacts may contact us directly to request to access information that we hold about them.
- *Right of portability*: You may export any of your lists, or selected information within any list, at any time by accessing your Mailchimp account.

Stricter Consent and Processing Requirements: You must lawfully obtain and process email addresses and other personal data from your subscribers and contacts.

- The personal data of your subscribers and 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 available now, so you can begin designing them to meet your specific GDPR compliance needs now.**
    - 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 are collecting.
    - While the information you collect via these forms is presumably being transferred to Mailchimp, it is *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 list sign-ups. Note that this may not be the default setting.
- The ability of your subscribers and 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 list, 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 of access* requirement.
        - Make sure that you are frequently updating any information stored within your Mailchimp account that relates to your subscribers or contacts, such as name and contact information, when requested to do so by a subscriber or contact.
- You should also ensure that you are keeping accurate records, especially of your subscribers' and contacts' consent permitting you to send them marketing emails, store and use their personal data, and any other processing activities which you are undertaking. Mailchimp can help you obtain proof of consent and will store a record of your subscribers'/contacts' consent in your Mailchimp account. When you use a Mailchimp signup form to add subscribers and 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, providing you with easy-to-access proof of consent.
- Keep in mind that any consent you obtain from your subscribers and contacts must comply with the GDPR requirements, irrespective of when that consent was obtained. However, Recital 171 of the GDPR indicates that you may continue to rely on any existing consent which meets the GDPR standards for consent. This means that it is not necessary to re-request consent from your subscribers or contacts when the GDPR goes into effect so

long as you met all of the requirements of the GDPR when you initially obtained consent. We recommend consulting with local counsel to determine if consents obtained prior to the GDPR comply with its requirements, or whether you should instead contact your subscribers and contacts to re-request consent in accordance with the GDPR requirements, or rely on a different lawful basis for your processing under the GDPR.

- You should review any Mailchimp integrations or add-ons that you are using (or plan to use), and any terms associated with those, to ensure that you have adequately disclosed potential data processing activities associated with your use of those services to your subscribers and contacts. For example:
    - *Connect Your Store, Google Web Retargeting Ads and Product Retargeting Emails*: If you choose to use the product retargeting email feature or the Google web remarketing ads feature, or if you have connected your e-commerce store to your Mailchimp account, your website may set a Mailchimp cookie which allows you to track certain activities of your subscribers. 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 these cookies and related pixels.
    - *Facebook Ads:* When you use certain options within Facebook's ad buying platform, such as the custom audience feature, a hashed value of your subscribers' email addresses may be transferred to Facebook. Only those email addresses you expressly select are hashed and transferred to Facebook. Mailchimp's Additional Terms of Use for Facebook and Instagram Ad Buying require anyone who is using the Facebook Ad Buying feature to get permission from their subscribers to transfer data to Facebook.
- 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 subscribers or contacts will be transferred to Mailchimp and processed by Mailchimp. For example, you may want to consider updating your privacy statement to include language that specifically identifies Mailchimp as one of your processors and delineates 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 of Mailchimp's 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 specific questions about the GDPR and your use of Mailchimp, you can email legal@mailchimp.com.

Last Updated: October 9, 2017