MailChimp FAQs
Update to Customer Data Protection Terms

Why have we changed our data processing agreement ("MailChimp DPA")?

On 25 May 2018, the EU will introduce a new data protection law called the General Data Protection Regulation ("**GDPR**"). The GDPR is a major overhaul of the current law under the existing Data Protection Directive (Directive 95/46/EC).

MailChimp is committed to GDPR compliance and to helping our customers comply with the GDPR when they use our services. We have updated the existing MailChimp DPA ("**Prior DPA**") to incorporate the mandatory data processor terms required by Article 28 of the GDPR ("**New DPA**"). We are pleased to offer all of our customers the New DPA.

More information about the GDPR, and MailChimp's compliance efforts, can be found in our GDPR guide, which is available here.

Am I required to sign the MailChimp DPA?

Yes. We require all customers who desire to retain a data processing agreement with MailChimp to sign the New DPA. The Prior DPA is not GDPR compliant, so it will not be effective moving forward and will be replaced by the New DPA.

Do I need to notify anyone that I am signing the New DPA?

If you have made commitments to any data subjects (like your subscribers) or data controllers (like your own customers) whose data you control or process, as applicable, you should consider reviewing any contracts in place with those persons or entities, as well as any publicly facing privacy statement or similar notices, in order to ensure that you are accurately representing the nature of the commitments that you have in place with your processors or sub-processors, such as MailChimp.

How does MailChimp comply with EU data export rules?

As a processor, MailChimp will be required under contract to ensure that any data transfers outside the EEA will be made in accordance with applicable law. To achieve this, MailChimp has certified to the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework (see our certification here).

In practice, this means that MailChimp in the U.S. is considered a "safe" recipient of personal data of its customers and their subscribers that is transferred from the EU and/or Switzerland to the U.S. by offering an "adequate level of protection" for such personal data (as determined by the European Commission). The Privacy Shield will remain an adequate data export mechanism under the GDPR (see Art 45(9)). Additional information regarding cross-border data transfers under the GDPR is included in our GDPR guide.

Do our customers need to sign model clauses with MailChimp, too?

No. As explained above, MailChimp has an active Privacy Shield certification, which covers all transfers of customer and subscriber personal data from the EU and/or Switzerland to MailChimp in the U.S. As a

result, our customers (existing and future) will not need to rely on or sign model clauses with MailChimp to lawfully transfer personal data to MailChimp in the U.S. Instead, they can rely on MailChimp's Privacy Shield certification.

What security measures does MailChimp apply to personal data?

MailChimp uses appropriate technical and organizational security measures to protect customer and subscriber personal data. MailChimp has an Information Security Management System (ISMS) and is regularly audited against SSAE 16 and PCI standards by independent third party auditors and internal auditors, respectively. MailChimp is also continually reviewing its safety measures for enhancements, including as part of its GDPR compliance program.

Can customers audit MailChimp's security measures?

MailChimp facilitates customer audits in a number of ways, as described in the New DPA:

- First, and on written request, MailChimp will provide its customers with a summary copy of its current audit report, so that its customers can verify MailChimp's compliance with the audit standards against which it has been assessed. As discussed above, MailChimp is regularly audited against SSAE 16 and PCI standards.
- Second, and also on written request, MailChimp will, no more than once a year, provide written responses (on a confidential basis) to all reasonable requests for information made by a customer, including responses to information security and audit questionnaires regarding MailChimp's compliance with security requirements and data protection laws.

MailChimp does not allow outside parties to perform penetration tests or onsite audits of the MailChimp application. However, MailChimp has a robust Information Security Management System to ensure the security of all customer and subscriber personal data, and conducts several audits throughout the year that provide assurances that MailChimp's controls are properly and securely managed.

I am a MailChimp user based in the U.S., and I am certified to the Privacy Shield Framework. I legally transfer personal data of my EU-based subscribers to the U.S. in reliance on that certification. Does the New DPA address my "onward transfer" obligations under the Privacy Shield?

Yes. See Section 8.2 (Privacy Shield) of the New DPA.

Where can I get more information?

If you have any questions or require assistance, please contact MailChimp's Legal Department at legal@mailchimp.com.