GDPR FAQ

Overview

What is the General Data Protection Regulation (GDPR)?

The GDPR is the European Union's new, comprehensive privacy and data protection law that took effect on May 25, 2018. The primary aim of the GDPR is to regulate how the personal data of individuals in the EU is processed – even by businesses that have no physical or legal presence in the EU. Organizations can face hefty fines for non-compliance: up to €20 million or 4 percent of annual global revenue, whichever is higher.

Take a look at our GDPR Readiness Guide to learn more or the full text of the GDPR articles.

Is Keap GDPR certified?

There is not yet any kind of recognized GDPR certification scheme, but we've been working hard to ensure that we're in compliance with the GDPR.

We now offer you (customers and Partners) a new Data Processing Addendum (DPA) inside of your account. Signing the DPA amends our standard terms of service to reflect obligations required by the GDPR. This is the instrument that legally binds us to complying with our responsibilities under the GDPR. It is available for review here: https://www.Keap.com/legal/dpa (but you'll still need to sign it within your account).

The new DPA governs the terms by which we, as a data processor, process data on behalf of you, our customers, (who are typically data controllers) in accordance with Article 28 of the GDPR.

According to Article 28 of the GDPR, data processors must act only upon the documented instructions of the data controller unless otherwise required by law. This, however, does not relieve us of any of our obligations or liabilities under the GDPR. We are still required to ensure that we're in compliance with the GDPR.

What is Keap doing to ensure that it (and its vendors) are compliant with the GDPR?

We've been re-papering vendor contracts and working with vendors to ensure they're fully GDPR compliant. We've also added a settings pane for you (our customers) to

provide us with the information required under Article 30(2) of the GDPR.

We'll continue to review our security measures, as we always do, to stay at the forefront of evolving industry standards and best practices.

We have also appointed a representative in the EU and an expert Data Protection Officer to help us ensure that we continue to live up to our own high standards for data protection and privacy.

GDPR and You

So Keap is compliant with the GDPR. Does that mean that I'm automatically compliant too? If not, where can I learn more about my own obligations?

No, while we've done our best to make it easier for you to be compliant, you'll still need to address your own practices regarding GDPR compliance. See more in our GDPR Readiness Guide .

Much of how you collect, use, and dispose of personal data is not determined by your data processor (that's us). Thus, each organization should get its own professional guidance on the topic to help ensure compliance. In addition to our Readiness Guide, here's an additional resource from the UK Information Commissioner's Office: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/.

Is Keap building new software features to help me comply with the GDPR?

Yes, we're releasing new features to help users manage their compliance with a number of key pain points in the law. This includes a set of features to help you manage the basis of processing (such as consent management) for your contacts, to make it easy to anonymize personal data (i.e., the right to be forgotten), and a customizable "block list" feature to help ensure that if someone asks you to never process their personal data, that their personal data can't be re-imported into your account. These features will help you to comply with many of your fundamental obligations under the GDPR.

Am I a data controller? Is Keap a data processor?

Typically, you (the Keap customer) will be considered a data controller (i.e., an organization that determines the purposes and means of the processing of personal data) and we will always be considered a data processor under the law.

Controllers and processors each have their own respective obligations under the law. Therefore, our GDPR compliance plan looks a bit different from what yours will look like. This doesn't mean we can't be used by data controllers – quite the opposite. When a data controller engages a service provider like us, the service provider is typically a data processor acting on behalf of the controller, and the processor acts at the behest of the controller. As stated above, our DPA will govern the relationship, and the nature of the processing activities, between Keap and its customers.

What is considered personal data?

According to GDPR Article 4 , personal data means..."any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

So, what does that mean for you?

Within your Keap account, that would include your customers' contact information. And they may at some point ask you to forget them, or modify their information to be accurate, etc. You would then be responsible for fulfilling that request.

Does the GDPR require an additional checkbox to be able to lawfully process personal data? Or will a sentence such as "enter your information for us to email you XYZ Pdf" be sufficient?

If you are processing personal data on the basis of the data subject's consent, you will need to include a mechanism to collect that consent, which could include an unticked checkbox which the data subject can tick to consent to the processing of his or her data. If you can consider this type of arrangement as a "contract" between you and the individual who requested the "something," then you may be able to skip the checkbox altogether, and base your processing on the need to perform your obligations under this "contract". See the Lawfulness of Processing section in the GDPR Readiness Guide.

If as customer asks me to exercise their Right to be Forgotten, do I have to remove them from my database?

Yes. Article 17 of the GDPR sets out the data subject's right to have his or her data erased (also known as the "right to be forgotten") when certain (broad) grounds apply, such as (without limitation) when the personal data are no longer necessary for the purposes of processing, where consent, as the sole basis of processing, has been withdrawn, or where the data subject has objected to the processing of his or her personal data and

you have no “compelling legitimate grounds” to continue the processing. It’s important to note how broadly this right applies: in practice, there will be few circumstances where the GDPR will not require the deletion of data at the data subject’s request.

Read more about the Right to be Forgotten in our GDPR Readiness Guide. See the Right to Erasure in the GDPR Readiness Guide.

What if I offer services free of charge (e.g. regularly emailing cat photos to my subscribed customers without requiring them to pay)? Does this constitute a contract, and can this be considered as a legal basis for lawful processing of personal data?

Yes. The GDPR is not limited to situations where money is transferred. According to Article 3.2(a) of the GDPR, merely offering goods or services to EU data subjects, even without payment, makes that transaction regulated by the GDPR. By using your services for which no payment is required, your customers typically agree to the Terms of Use/Terms of Service that you display on the website, thus forming a valid contract. You can use this as a legal basis for justifying the processing of personal data, simply because it is necessary for fulfilling your obligations under the contract. Without knowing your customers’ email, how else would you be able to share cat photos with them? Read more about the Lawfulness of Processing in our GDPR Readiness Guide.

If I have an EU Representative based in the United Kingdom (UK). Will that still work (after Brexit)?

No. Post-Brexit, a representative located in the UK will no longer lawfully be considered a representative in the EU, within the meaning of Article 27 of the GDPR. With that being said, it’s important to remember the UK will remain a Member State of the EU until the date of its formal withdrawal, whenever that may be ultimately be.

Consent

Do I need to obtain consent again from all my contacts?

Not necessarily. There are other permitted bases for processing personal data under Article 6 of the GDPR, such as the need to process personal data for the performance of a contract, or the legitimate interests of the data controller or another party. However, if you will be processing personal data based solely on the consent of the individual, you likely need to re-acquire consent from these “old” contacts. For more information on this topic, take a look at the Consent section of our GDPR Readiness Guide.

Under GDPR, can I still have my opt-in forms checked by default?

No, please note that the use of pre-ticked opt-in boxes is not valid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely using a service (without first ticking a box to indicate agreement) doesn't count as "consent".

What is considered legal processing of customer data?

The categories or basis of processing are the following:

1. consent of the data subject;
2. processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;
3. processing is necessary for compliance with a legal obligation to which the controller is subject;
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Check out this blog post on the issue: https://www.Keap.com/product-blog/gdpr-article-6

Data Protection

Who is Keap's Data Protection Officer (DPO)?

Our DPO is: Matthew Joseph, CIPP/EU

https://keap.com/legal/data-protection-faq/en#dpoContactFormModal

In accordance with Article 38 of the GDPR, members of the public may contact the DPO with regard to issues related to processing of their personal data and to exercise their rights under the GDPR – for example, to object to the processing of their data in cases where the data controller (that's you, the Keap customer) does not provide an adequate

response.

Who is Keap's representative in the European Union pursuant to Article 27 of the GDPR?

Our Article 27 Representatives are:

Matthew Joseph, CIPP/EU
Klimentská 46,
Prague 1, 11000
Czech Republic
Email: experts@verasafe.com

VeraSafe Ireland LTD
Unit 3D North Point House
North Point Business Park
New Mallow Road
Cork 123AT2P
Ireland
Email: experts@verasafe.com

In accordance with Article 27 of the GDPR, supervisory authorities and persons whose personal data are being processed by us, Keap, may contact VeraSafe (our Article 27 Representative) on all issues related to processing, for the purposes of ensuring compliance with the GDPR.

If a business is marketing to people in the EU, do they need to have an EU Representative?

Yes. If you are offering goods and services to people in the EU, for free or for a fee, and thus processing their data, in most cases, you will need to appoint an EU representative, as required by Article 27 of the GDPR. For example, our GDPR Article 27 representative in Europe is VeraSafe Ireland Ltd.

What solution does Keap offer for cross-border data transfers?

Under the GDPR, personal data may only be transferred outside the European Economic Area (commonly referred to as the EEA and which consists of the EU, plus Norway, Iceland, and Liechtenstein) in certain circumstances, such as to a country whose data protection laws are deemed "adequate" by the European Commission, or by relying on an approved data transfer mechanism.

Because we're outside of the EU, we currently offer customers the EU Model Contract (the alternative to Privacy Shield, which comes from the EU and is provided by the FTC)

to enable the lawful flow of personal data from the EEA to Keap in the United States.

The EU Model Contract contains standard contractual clauses which are approved by the European Commission, and which govern the lawful transfer of data from the EEA to countries outside of the EEA. Under the GDPR, additional legitimate methods of exporting personal data outside the EEA may be introduced. In the event of any changes to or new rules associated with the GDPR, Keap will review and respond appropriately.

What security controls has Keap implemented to safeguard my data?

Our Data Security Statement goes well beyond the customary confidentiality clauses found in the business terms of many SaaS providers. The statement describes some of the specific data security controls that we've implemented and, by publishing the information, legally obligates us to maintain the high standard of data security that's described in the Statement.

The Data Security Statement can be found here: https://www.Keap.com/legal/data-security

Is Keap PCI Compliant?

We adhere to, and are audited annually for compliance with, the Payment Card Industry Data Security Standard, which is a rigorous data protection framework oriented towards the protection of payment card data.

Our most recent PCI DSS audit documentation is available upon request. Please contact pci@Keap.com if you require the documentation.

GDPR and Other Channels

How does the GDPR apply to social media?

The GDPR applies to personal data processed for the purposes of social media marketing campaigns, communication with customers via social media, and using Facebook tracking pixels and similar technologies. However, the specific impact depends on the manner in which the social media is used. Social media isn't specifically discussed in the GDPR, so there are no aspects of the GDPR that are unique to social media or social media marketing.

Does the GDPR apply only if a customer buys something from a website?

If you are offering services to a data subject in the EU, they do not necessarily need to buy something from you in order for the GDPR to apply. When you go out of your way to offer goods or services to the people in the EU, the GDPR likely applies to you.

In terms of vendors, how does this apply with third-party integrations with Keap? If Keap is GDPR compliant but a third-party software is used (i.e. Zapier, Parsey or anything else), that 3rd party technically has access to the contact record information.

When you configure your Keap service to connect with those third-party apps, you should ensure that those vendors are also GDPR compliant, and that your relationship with that vendor meets the requirements laid out in Article 28 of the GDPR. For example, the service agreement in place between your company and the third-party service provider should impose various obligations on that service provider, such as a requirement to use the personal data only upon your instructions, and to notify you of any data breaches.