GDPR

Everything you need to know
What is GDPR?

GDPR (General Data Protection Regulation) is Europe’s new privacy law. Adopted in April 2016, it replaces the 1995 Data Protection Directive – and marks the biggest change in data protection in 20 years.

On May 25, 2018, the new law came into force across the EU. And businesses need to change the way they handle your data.

Why is GDPR so important?

In recent years, the amount of data created and stored around the world has skyrocketed. GDPR aims to address that challenge, by making cross-border business easier and more transparent. It will also give you more control over your data and how it’s used.

Our guide is designed to help you understand what GDPR is and how it affects you. You’ll also see examples and tips to review your marketing materials, so you can show contacts you take their data security seriously.

So while you get more rights to guard your data, businesses have to follow new rules in the way they manage it.

This guide is for informational purposes only. Please do not treat it as a substitute of a professional legal opinion. Always consult your lawyer or other professionals responsible for data protection within your organization. The information contained herein is subject to change without notice and is not warranted to be error-free. Please note that GetResponse uses its best efforts to ensure that this guide is complete, relevant and includes correct information, however, GetResponse will not bear any responsibility for guide’s accuracy, completeness or its fitness for any purpose. Any reliance on any information contained in this guide is solely at your own risk. In no event shall GetResponse be liable for any indirect, special, incidental or consequential damages arising out of any use of or reliance on any content or materials contained herein.
Let’s start with some definitions

Are you affected by the regulations?
To find out, let’s start with the definitions you’ll spot in the privacy laws and our guide.

Personal data

Your personal data is any information that relates to you. It covers your name, location data, and contact details. It also spans numbers that identify you – and other information about your physical, physiological, genetic, mental, economic, cultural or social identity.

Photos, movies and recorded voices are all examples of personal data – as are your email addresses, IP address, cookie identifiers and many other things that can be used to identify you.

Data processing

You process personal data when you deal with it in any way – either manually or with automation. Here are some examples:

- Collecting and storing data
- Recording, organizing, and structuring data
- Erasing or destroying data
- Changing, disclose, sending, making it available, or using it in any other way

So, processing is anything you do with any personal data.

Data controller

Do you decide why and how personal data is processed? Then you’re a data controller.
Let’s say you run an online store, and use a customer database to send orders or marketing emails. In this way, you control customers’ personal data – and your customers are data subjects.

Data processor

Do you process personal data on behalf of the controller? Then you’re a data processor. Let’s say you decide to hire a marketing agency to promote your online store. You give the agency access to your database, so they can send communications on your behalf. That makes them the data processor.

If you upload your contact list to GetResponse, we become the processor of that personal data.
Does GDPR affect me?

GDPR may apply if you’re a **data controller** or **data processor**:

1. based in the EU, even if you process data outside the EU.
2. based outside the EU, but process personal data of EU residents. This applies if you sell goods or services (or offer them for free), or monitor people's behavior within the EU.

How do you know if you offer goods or services to people in the EU?

- You use a language or currency common in one or more EU countries, to help people who live there take up your offer.
- You mention customers or users who are in the EU.
- You clearly target your offer to people in the EU.

In this case, you'll need to comply with GDPR.

On the other hand, you probably won't need to comply if you simply have a website, email address, or other contact details that can be accessed in the EU – and the language is common to your country (and not to any EU member state).
It's worth keeping in mind that before GDPR, you still had to meet regulations when processing personal data.

GDPR simply means data controllers must make a greater effort to process personal data within the law. They also have to make it clear how data will be processed – and ask for consent.

Unlike past laws, GDPR also refers directly to data processors – and outlines how they must now comply. And if there’s a personal data breach, they need to notify the data controller who needs to notify supervisory authorities and data subjects as soon as possible.

If you have a GetResponse account, you’re the controller of your contacts’ personal data. That's because you decide why and how their information will be used. And that means you’re responsible and liable under GDPR.

**What happens if I don’t comply?**

There are two levels of fines for breaching GDPR:

- **Up to 2% of global annual turnover or €10 million (whichever is higher).** This covers infringements related to security and data breach notification, certification, and cooperating with the supervising authority.
• Up to 4% of global annual turnover or €20 million (whichever is higher). This covers infringements related to the basic principle for processing data. Such as conditions for consent, data subjects' rights, and transferring personal data to third countries.

Supervisory authorities also have the power to place limits on data processing. They can ban the controller from using data – or order them to provide certain information.

How does GetResponse comply with GDPR?

We’ve always taken your data security seriously. And we observe all European laws, especially those that safeguard personal data. In fact, we adopted our GDPR Compliance Implementation Plan more than a year before the law went into effect.

As an online marketing leader, we’re an active member of industry organizations focused on data privacy, GDPR, and how it applies to businesses and media. We observe negotiation of codes of conduct with regulatory authorities – and plan to implement an approved code or certification in the near future.

Beyond that, we carefully weigh up recommendations made by data protection bodies, as well as the Article 29 Working Party on the protection of individuals. And because our platform is available worldwide, we do our best to keep an eye on regulations outside the EU.

When getting ready for GDPR, we planned how to best support our customers – and the people whose personal data they process. We publish information and updates on new data processing rules, and showcase how we’re helping keep our customers compliant.

Which is why we developed the Consent fields tool (formerly known as GDPR fields) in all GetResponse accounts to help our customers be both compliant with GDPR and transparent with their customers regarding opt-in transparency and data processing.

For us, the new regulations aren't a hurdle. We see them as a chance to serve you even better – and continue keeping your data safe. And we'd love to see all our customers do the same for their contacts.
How to get your account ready

First, review your signup processes and marketing materials now. See what work you need to do inside or outside GetResponse.

Let’s look at some GDPR obligations in more detail, how they might apply to your account, and how you can use GetResponse Consent fields (formerly known as GDPR fields) to help you obtain and manage your contacts’ consent.

Getting consent

You’ll need to ask your contacts if it’s OK to process their personal data. The GDPR defines consent as:

“Any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”

This bit’s important: they need to explicitly give their consent – and you can’t make it a pre-condition for providing a service (unless you need that information to carry out the service). You also need to prove they have opted in.

It should be easy for contacts to withdraw consent. And you’ll need to stop processing their data if you have no other legal reason to do so.

Before collecting personal data, you need to tell the person:

• Who you are and your contact details
• Why and how you will use their data – and the legal basis for doing so
• If their personal data will be shared with anyone else
• If you plan to transfer their data to a third country or international organization, as well as the relevant safeguards and how they can view them

You also need to share:

• How long you’ll keep their data
• Their rights to access, update, or erase it – or stop you from processing it
• How they can withdraw their consent
• How they can lodge a complaint with a supervisory authority
• Why you need the personal data. Is it a statutory or contractual requirement? Is it needed to enter into a contract? Do they need to provide their personal data? What happens if they don't?
• Whether you use profiling, the logic used and the significance or consequences of processing their data in that way.

Above all, new contacts should know exactly how you’ll use the data they give you.
How can you prove you have their consent?

Using our Consent Fields tool you can create consent fields that you can populate on your GetResponse signup forms, landing pages, and webinars to obtain consent from your subscribers when they join your list.

Please note that the above examples of a Consent field name and description should be filled in with a text that adequately corresponds to the data processing activities you plan to carry out and by no means should serve as a template to be used in your actual activity.
You can then manage and view your contacts' consent as a detailed log related to each consent field they have opted in under.

Check out our FAQs to learn more about using Consent fields on your signup materials to obtain consent.

The right to be forgotten

If a contact asks you to erase their personal data, you must do it as soon as possible – if you have no legal grounds to keep processing it. You also should delete their data if you no longer need it, if it was used unlawfully, or if the contact exercised their right to object.

In your GetResponse account, you'll find three options to help you comply:

1. Your contacts can unsubscribe from your list(s) in any sent message. An unsubscribe link is automatically added to each message footer. For more, see how can a contact unsubscribe from my list and updating footer links.
2. You can remove contacts from your list, if they ask you directly. See how to remove them from your lists or entire account.

3. You or your contacts can ask our customer support to remove them. Get us 24/7 on LiveChat or email us.

If another data processor (such as third-party services) has the contact's information, you should also ask them to erase it – or do it yourself.

**The right to object**

Contacts can object any time to you using their personal data for direct marketing purposes, or for legitimate interests such as:

- Your internal administrative activities.
- Ensuring network and information security (providers of electronic communications networks, security technologies, and related services).
- Preventing fraud.

To comply, just follow the steps we mentioned in the previous section.
The right to rectification

Under GDPR, your contacts can also ask you to update their personal data, if it’s incorrect or incomplete. And you should do it straight away.

Here’s how:

- Your contacts can view and update their data that you have in your GetResponse account. They can simply click on the “Change contact details” link automatically included in the footer of your sent messages.
• You can update their data in your account at any time. Just go to Contacts, search for their name, click on it, and edit the custom fields. You just can't change their email address and opt-in proof.

• You or your contacts can ask GetResponse customer support to edit their data. Get us 24/7 on LiveChat or email us.

**The right of access**

Your contacts also have the right to know:

• If their data is being used
• How they can access it
• Why it's being used
• Who it's shared with
• How long it will be stored

You should also let them know how they can change or erase their data – or restrict the way you process it.
To comply, you can follow the steps in the “Right to rectification” section. Plus:

- You can export a contact’s details at any time and send it to them in a CSV, XLS, or XML file.

Questions or concerns?

You can email our privacy experts directly with any questions.

2. **Sensitive personal data** – special categories of personal data which is, by its nature, particularly sensitive in relation to fundamental rights and freedoms and merits specific protection as the context of its processing could create significant risks to the fundamental rights and freedoms. This type of personal data includes:
   - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,
   - genetic data,
   - biometric data for the purpose of uniquely identifying a natural person, data concerning health,
   - data concerning a natural person’s sex life or sexual orientation.

   Such personal data should not be processed, unless processing is allowed in specific cases set out in GDPR.

3. **Data processing** – 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;

4. **Data controller** – the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

5. **Data processor** – a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.