What is GDPR, the EU's new data protection law?

What is the GDPR? Europe's new data privacy and security law includes hundreds of pages' worth of new requirements for organizations around the world. This GDPR overview will help you understand the law and determine what parts of it apply to you.

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

With the GDPR, Europe is signaling its firm stance on data privacy and security at a time when more people are entrusting their personal data with cloud services and breaches are a daily occurrence. The regulation itself is large, far-reaching, and fairly light on specifics, making GDPR compliance a daunting prospect, particularly for small and medium-sized enterprises (SMEs).

We created this website to serve as a resource for SME owners and managers to address specific challenges they may face. While it is not a substitute for legal advice, it may help you to understand where to focus your GDPR compliance efforts. We also offer tips on privacy tools and how to mitigate risks. As the GDPR continues to be interpreted, we'll keep you up to date on evolving best practices.

If you've found this page — "what is the GDPR?" — chances are you're looking for a crash course. Maybe you haven't even found the document itself yet (tip: here's the full regulation). Maybe you don't have time to read the whole thing. This page is for you. In this article, we try to demystify the GDPR and, we hope, make it less overwhelming for SMEs concerned about GDPR compliance.

History of the GDPR

The right to privacy is part of the 1950 European Convention on Human Rights, which states, "Everyone has the right to respect for his private and family life, his home and his correspondence." From this basis, the European Union has sought to ensure the protection of this right through legislation.

required to be compliant.

Scope, penalties, and key definitions

First, if you process the personal data of EU citizens or residents, or you offer goods or services to such people, then **the GDPR applies to you even if you're not in the EU**. We talk more about this in another article.

Second, the **fines for violating the GDPR are very high**. There are two tiers of penalties, which max out at €20 million or 4% of global revenue (whichever is higher), plus data subjects have the right to seek compensation for damages. We also talk more about GDPR fines.

The GDPR defines an array of legal terms at length. Below are some of the most important ones that we refer to in this article:

Personal data — Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. Pseudonymous data can also fall under the definition if it's relatively easy to ID someone from it.

Data processing — Any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing... so basically anything.

Data subject — The person whose data is processed. These are your customers or site visitors.

Data controller — The person who decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you.

Data processor — A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations. They could include cloud servers like Tresorit or email service providers like ProtonMail.

What the GDPR says about...

For the rest of this article, we will briefly explain all the key regulatory points of the GDPR.

Data protection principles

If you process data, you have to do so according to seven protection and accountability principles outlined in Article 5.1-2:

1. **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject.
2. **Purpose limitation** — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
3. **Data minimization** — You should collect and process only as much data as absolutely necessary for the purposes

The GDPR says data controllers have to be able to demonstrate they are GDPR compliant. And this isn't something you can do after the fact: If you think you are compliant with the GDPR but can't show how, then you're not GDPR compliant. Among the ways you can do this:

- Designate data protection responsibilities to your team.
- Maintain detailed documentation of the data you're collecting, how it's used, where it's stored, which employee is responsible for it, etc.
- Train your staff and implement technical and organizational security measures.
- Have Data Processing Agreement contracts in place with third parties you contract to process data for you.
- Appoint a Data Protection Officer (though not all organizations need one — more on that in this article).

Data security

You're required to handle data securely by implementing "appropriate technical and organizational measures."

Technical measures mean anything from requiring your employees to use **two-factor authentication** on accounts where personal data are stored to contracting with cloud providers that use **end-to-end encryption**.

Organizational measures are things like **staff trainings**, adding a **data privacy policy** to your employee handbook, or **limiting access to personal data** to only those employees in your organization who need it.

If you have a data breach, you have 72 hours to tell the data subjects or face penalties. (This notification requirement may be waived if you use technological safeguards, such as encryption, to render data useless to an attacker.)

Data protection by design and by default

From now on, everything you do in your organization must, "by design and by default," consider data protection. Practically speaking, this means you must consider the data protection principles in the design of any new product or activity. The GDPR covers this principle in Article 25.

Suppose, for example, you're launching a new app for your company. You have to think about what personal data the app could possibly collect from users, then consider ways to minimize the amount of data and how you will secure it with the latest technology.

When you're allowed to process data

Article 6 lists the instances in which it's legal to process person data. Don't even think about touching somebody's personal data — don't collect it, don't store it, don't sell it to advertisers — unless you can justify it with one of the following:

1. The data subject gave you specific, **unambiguous consent** to process the data. (e.g. They've opted in to your marketing email list.)
2. Processing is necessary to execute or to prepare **to enter into a contract** to which the data subject is a party. (e.g. You need to do a background check before leasing property to a prospective tenant.)
3. You need to process it **to comply with a legal obligation** of yours. (e.g. You receive an order from the court in your jurisdiction.)

reason, and notify the data subject.

Consent

There are strict new rules about what constitutes consent from a data subject to process their information.

- Consent must be "freely given, specific, informed and unambiguous."
- Requests for consent must be "clearly distinguishable from the other matters" and presented in "clear and plain language."
- Data subjects can withdraw previously given consent whenever they want, and you have to honor their decision. You can't simply change the legal basis of the processing to one of the other justifications.
- Children under 13 can only give consent with permission from their parent.
- You need to keep documentary evidence of consent.

Data Protection Officers

Contrary to popular belief, not every data controller or processor needs to appoint a Data Protection Officer (DPO). There are three conditions under which you are required to appoint a DPO:

1. You are a public authority other than a court acting in a judicial capacity.
2. Your core activities require you to monitor people systematically and regularly on a large scale. (e.g. You're Google.)
3. Your core activities are large-scale processing of special categories of data listed under Article 9 of the GDPR or data relating to criminal convictions and offenses mentioned in Article 10. (e.g. You're a medical office.)

You could also choose to designate a DPO even if you aren't required to. There are benefits to having someone in this role. Their basic tasks involve understanding the GDPR and how it applies to the organization, advising people in the organization about their responsibilities, conducting data protection trainings, conducting audits and monitoring GDPR compliance, and serving as a liaison with regulators.

We go in depth about the DPO role in another article.

People's privacy rights

You are a data controller and/or a data processor. But as a person who uses the Internet, you're also a data subject. The GDPR recognizes a litany of new privacy rights for data subjects, which aim to give individuals more control over the data they loan to organizations. As an organization, it's important to understand these rights to ensure you are GDPR compliant.

Below is a rundown of data subjects' privacy rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

Ben Wolford
Editor in Chief, GDPR EU

A journalist by training, Ben has reported and covered stories around the world. He joined ProtonMail to help lead the fight for data privacy.

GDPR can be found here. Nothing found in this portal constitutes legal advice.

Getting Started

What is GDPR?

What are the GDPR Fines?

GDPR Compliance Checklist

Templates

Data Processing Agreement

Right to Erasure Request Form

Writing a GDPR-compliant privacy notice

Technical Review

Data Protection Office Guide

GDPR and Email

Does GDPR apply outside of the EU

About Us

GDPR.eu is co-funded by the Horizon 2020 Framework Programme of the European Union **and operated by Proton Technologies AG.**

GDPR Forms and Templates

Data Processing Agreement > Right to Erasure Request Form > Privacy Policy >