

FAQs about the GDPR

Last Modified on Apr 30, 2020

The General Data Protection Regulation (GDPR) is the most significant privacy regulation in years. Below we have consolidated some of the most frequently asked questions to help you understand the impact of the regulation.

When did the GDPR come into effect?

The GDPR took effect on May 25, 2018. The legislation was approved and adopted by the European Parliament in April 2016, and is recognized as a law in all EU member states. The two-year transition period was to allow member states to ensure the law is fully implementable at the time it goes into effect.

Who does the GDPR affect?

The GDPR applies to all organizations that offer products or services to, or monitor the data of EU residents. This includes organizations located outside of the EU that may have prospects or customers who are EU residents. Additionally, the regulation applies to B2B service providers that process data on behalf of organizations.

What are the penalties for non-compliance?

Organizations that do not comply can be fined up to 4% of annual global turnover or €20 million, whichever is higher. This is the maximum fine that can be imposed for the most serious infringements. For smaller infringements, the GDPR imposes smaller fines. For example, a company can be fined 2% for not having their records in order, not notifying the supervising authority and data subject about a breach, or not conducting impact assessments.

What constitutes personal data?

Any information that can be used to identify an individual. This includes data directly linked to a person, such as their name, identification number, location, or any online identifier. Personal data can also be indirectly linked to an individual, including physical, physiological, genetic, mental, economic, cultural, or societal information

What is the difference between a data processor and a data controller?

A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller.

Does my business need to appoint a Data protection officer (DPO)?

Your organization may need to appoint a DPO if you are in the public sector, if you regularly and systematically monitor data subjects on a large scale, or if you process sensitive data on a large scale. Your DPO can either be an employee of your organization, or be retained as a contracted service. If your organization doesn't fall into one of these categories, then you do not need to appoint a DPO. [Learn more about the requirement to appoint a DPO](#)

Do I have to get explicit consent from my data subjects?

The GDPR requires that you have a "legal basis for processing," meaning a legal right for collecting, storing, or accessing data belonging to a specific person. Explicit consent from the data subject is one way to establish a legal basis for processing. With online scheduling, because the activity is customarily initiated by customers, a lawful basis for processing can usually be obtained without consent. Under the GDPR you can process information if it is

necessary to fulfill a business obligation to a prospect or customer. When a prospect or customer initiates scheduling, this creates a business obligation for you to conduct the requested meeting. For most organizations, this should be enough to ensure a lawful basis for processing information via OnceHub without requesting consent. [Learn more about lawful bases for processing](#)

To learn more about OnceHub's compliance with the GDPR, read our ebook: [A practical guide to using OnceHub in a GDPR compliant manner](#)
