**What is the GDPR?**

The General Data Protection Regulation (GDPR) is an EU-wide regulation that controls how companies and other organizations handle personal data. It is the most significant initiative on data protection in 20 years and has major implications for any organization in the world, serving individuals from the European Union.

To give people control over how their data is used and to protect “fundamental rights and freedoms of natural persons”, the legislation sets out strict requirements on data handling procedures, transparency, documentation and user consent.

*Any organization must keep record of and monitor personal data processing activities.*

As data controller, any organization must keep record of and monitor personal data processing activities. This includes personal data handled within the organization, but also by third parties – so called data processors.  
  
Data processors can be anything from Software-as-a-Service providers to embedded third party services, tracking and profiling visitors on the organization’s website.

Both data controllers and processors must be able to account for what kind of data is being processed, the purpose of the processing and to which countries and third parties the data is transmitted.

If personal data is being sent to organizations or jurisdictions beyond the reach of the GDPR or that are not deemed ‘adequate’ by the GDPR, one must inform the user specifically about this and the risks involved.

*All consents must be recorded as evidence that consent has been given.*

On May 4, 2020, the [**European Data Protection Board (EDPB)**](https://edpb.europa.eu/) adopted guidelines on valid consent under GDPR.

Valid consent must be a freely given, specific, informed and unambiguous indication of the user’s wishes, i.e. a clear and affirmative action by the user.

The [**EDPB guidelines**](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf) make it clear that **scrolling or continued browsing on a website does not constitute valid consent** and that **cookie banners are not allowed to have pre-ticked checkboxes**.

**Cookie walls (forced consent) are also ruled non-compliant.**

EDPB is the highest supervisory authority in charge of the application of the GDPR across the EU and is comprised of representatives from the data protection authorities of each EU member state. Their guidelines and decisions form the bases of enforcement of the GDPR on a national level.

[**Learn more about EDPB guidelines on valid consent**](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf)

Individuals now have the “right of data portability”, the “right of data access” along with the “right to be forgotten” and can withdraw their consent whenever they want. In such case the data controller must delete the individual’s personal data if it’s no longer necessary to the purpose for which it was collected.

In case of a data breach, the company must be able to notify data protection authorities and affected individuals within 72 hours.

Furthermore, GDPR imposes an obligation on public authorities, organizations with more than 250 employees and companies processing sensitive personal data at a large scale to employ or train a data protection officer (DPO). The DPO must take measures to ensure GDPR compliance throughout the organization.

In relation to Brexit, the UK Government plans to implement equivalent legislation that will largely follow the GDPR.

**What does the GDPR mean for my website?**

If your website is serving individuals from the EU and you – or embedded third party services like Google and Facebook – are processing any kind of personal data, you need to obtain prior consent from the visitor.

To obtain valid consent, you need to describe the extent and purpose of your data processing in plain language to the visitor, prior to processing any personal data.

This information must be available to the visitor at all times, e.g. as part of your privacy policy. You must also make available an easy way for the visitor to change or withdraw consent.

All consents must be logged as proof and all tracking of personal data, also by embedded third party services, must be documented, hereunder to which countries data is transmitted.

Check out the [**EU-infopage**](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en/) on the reform of the data protection laws.

See also their infographic [**Data Protection – Better rules for small business**](https://ec.europa.eu/justice/smedataprotect/index_en.htm)

**How PPDM CMP helps**

Using [**PPDM Consent Management Platform (CMP)**](https://www.cookiebot.com/?utm_source=bing&utm_medium=cpc&utm_campaign=uk-generic&utm_device=c&utm_term=privacy+policy+for+website&utm_content=uk-eng-privacy-policy), you can automate GDPR compliance for your website on the requirements regarding tracking and consent.

PPDM CMP enables you to monitor and document any kind of tracking on your website, display the relevant information to your website visitors and automatically obtain and log all user consents.

**What is the definition of personal data?**

The GDPR defines personal data as “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.”

Online identifiers such as IP addresses now qualify as personal data, unless anonymized.

Pseudonymized personal data is also subject to the GDPR, if it by reverse engineering is possible to identify whose data it is.

**GDPR enforcement date: 25th of May 2018**

The EU data protection reform was adopted by the European Parliament and the European Council on April 27th, 2016. The European Data Protection Regulation is applicable as of May 25th, 2018, and replaces the Data Protection Directive.

**GDPR Fines and Penalties**

Organizations in non-compliance risk heavy fines of up to €20 million, or 4% of the organization’s global yearly turnover, whichever is higher.

**GDPR checklist: 6 things I need to do**

**1. Prepare your organization:**

Introduce stakeholders across your organization to the requirements of GDPR. Conduct employee training in Cyber Security, Privacy by Design and Privacy by Default principles. Assign a Data Protection Officer (DPO) if required, i.e. if you employ more than 250 people.

**2. Audit your data:**

Make sure you know where all your data lives, who has access and on what devices. Identify where personal data is processed, including by third party processors. Document the grounds for lawful processing and update current privacy policies.

**3. Audit service partners:**

Make sure that service partners, i.e. embedded third party services on your website or Software-as-a-Service providers, are also compliant with GDPR, or under an officially sanctioned data jurisdiction. Review and map their international data flows.

**4. Obtain consent:**

Implement methods for seeking, obtaining and recording consent to ensure compliance. Keep a clear record of what each individual data subject consented to and provide options for the data subject to revoke or change a consent.

**5. Respond to data rights:**

Implement procedures that enables your organization to respond to data subject rights, i.e. data access, rectification and erasure. Document how they will be exercised in both customer and employee contexts.

**6. Prepare for data breaches:**

Ensure that there are procedures in place to detect, investigate and report on personal data breaches to meet the GDPR’s 72 hour-deadline for notification.

**GDPR compliance and requirements**

**GDPR Courses, Training and Certification:**

You can achieve the EU GDPR Foundation (EU GDPR F) and EU GDPR Practitioner (EU GDPR P) qualifications (both ISO 17024-accredited) on various courses from i.e. [**IT Governance**](https://www.itgovernance.eu/shop/product/certified-eu-general-data-protection-regulation-gdpr-foundation-and-practitioner-combination-course/). The International Association of Privacy Professionals (IAPP) also provides [**online training**](https://iapp.org/store/trainings/a191a000001kuXQAAY/).