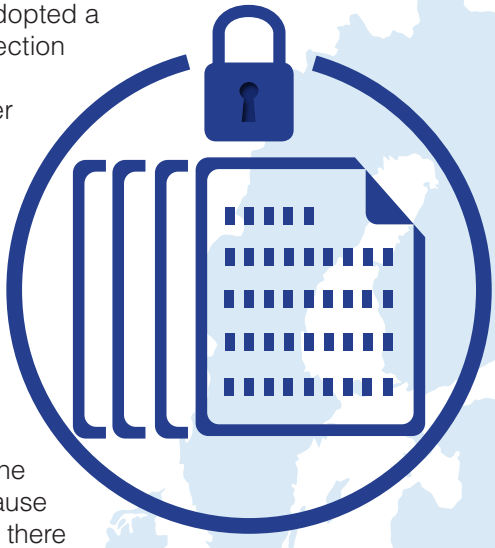
The European Union's GDPR General Data Protection Regulation

What is the GDPR?

On April 8, 2016, the European Union (EU) adopted a new regulation called the "General Data Protection Regulation" (GDPR). It replaces the EU Data Protection Directive and applies to all member countries without the need for national legislation. After four years of discussion and amendments, the regulation officially takes effect on May 25, 2018, and places the EU at the forefront of data protection standards.



What does the GDPR do?

The EU Data Protection Directive, established in 1995, was a great step towards protecting the personal information of EU residents, but because it wasn't normalized across all member states, there were inconsistencies that made it difficult for organizations to operate in multiple states. The GDPR addresses that shortfall by defining specific standards for the protection of data as required for all data controllers, regardless of location. Ultimately, the end-goal of the GDPR is to make regulation easy for data controllers around the world to follow while also maximizing the protection of data for EU residents.

What is personal data?

Article 4 of 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."

What does the GDPR require of organizations?

In order to comply to the full scope of the GDPR, it is recommended that organizations seek legal counsel. At a minimum, here are a few high-level action items:

- **Get consent**. A data controller must be able to prove that consent was given by the data subject.
- Conduct a data protection impact assessment. It's important to **assess privacy risks** of processing personal data of individuals.
- **Appoint a data protection officer**. This person is responsible for overseeing compliance and data protection strategies.
- Be prepared to **report data breaches**. Under the GDPR, organizations must report a breach within 72 hours.
- **Maintain records of processing**. Article 30 states that controllers "shall maintain a record of processing activities under its responsibility" and defines seven types, which can be found here: **https://gdpr-info.eu/art-30-gdpr**.

Failure to Comply

Organizations that fail to comply will face significant fines—as high as four percent of the organization's annual revenue. Furthermore, individuals may take action against any entity that improperly handles their personal data.

KnowBe4
Human error. Conquered.