

COMPLIANCE BRIEF

General Data Protection Regulation (GDPR)

Giving citizens control of their personal data

What is the GDPR and Why It's Important

The primary objectives of the General Data Protection Regulation (GDPR) are to give citizens and residents back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the European Union (EU).

Although the GDPR is legislation originating from the EU, its *scope* and *impact* is *global*. Any enterprise that provides a service whereby personal data of a resident of the EU is processed will be impacted by GDPR requirements, regardless of where the enterprise is located and conducts business.

However, there are a number of specific requirements that are brand new and which firms need to be aware of:

- Consent from individuals to process their personal data must be granted
- Personal data being processed may need to be encrypted
- Individuals have a right to be told what personal data of theirs is being processed, and for what reason
- Individuals can request at any time that any organization cease to process their personal data and delete any record of it
- Data breaches need to be reported to the applicable supervisory authority within 72 hours
- Data subjects may also need to be notified that their data has been compromised, which could result in severe reputational damage

WHAT DO YOU NEED TO KNOW?

Given the current regulatory environment – not least the long-standing Data Protection Directive - many of the demands of GDPR will have already been met. From appointing a CISO to adopting a written cybersecurity policy, good security practices will address a large part of the GDPR requirements.

CIVIL PENALTES

Organizations can be fined up to €20,000,000 or 4% of their global annual revenue (whichever is greater).

WHAT SHOULD YOU DO NEXT?

- Ensure your organization has a Data Protection Officer appointed to take overall responsibility for GDPR compliance
- Ensure your organization's privacy policy is up to date to meet the stringent requirements of GDPR. This should provide clear information regarding how you are processing personal data, and how you are using it
- Ensure your process for obtaining consent to process a customer's data is up to date and that a record is kept regarding how and when such consent was obtained.
- Ensure that *all* staff are sufficiently trained to deal with any data subject access requests or other requests from data subjects around their personal data
- Audit any personal data that the company processes to ensure that it's accurate, up to date and that the company still has a legal basis to retain it
- Ensure your organization is set up and trained to deal with any data breaches and reporting of such to the data protection authorities

A copy of the GDPR can be found here: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>

2



Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1(888)833-1142
Fax: 1(412)262-2574

info@certesnetworks.com
sales@certesnetworks.com

We offer an encryption solution that is simple, scalable and uncomplicated.