RAPID7

QUICK GUIDE

What You Need to Know About the **General Data Protection Regulation (GDPR)**

The General Data Protection Regulation (GDPR) regulates the privacy and handling of European Union (EU) citizens' personal data. GDPR replaces the existing EU Data Protection Directive, and unifies data protection laws across the EU with a single set of rules.

Key Changes

Key changes that may impact organisations include:

- **Privacy-by-design** – Data protection must built into business processes and systems from the start and provided by default.
- **Data retention** – Personal data should only be kept for as long as is necessary, then the data must be securely destroyed or anonymised.
- **Right to be forgotten** – Users are able to request for their data to be deleted; they can also request for a copy to be sent to a third party.
- **Mandatory breach notification** – Any breaches of personal data must be reported to Supervisory Authorities within 72 hours of discovery, and depending on the extent of the breach, to affected Data Subjects without delay.
- **Penalties for non-compliance** – Fines up to 4% of a company's annual worldwide turnover or €20million, whichever is higher.

Common Questions

What is Personal Data?

Any information which can directly or indirectly identify a 'natural person', whether it's to do with their private, professional, or public life. This includes their name, birth date, email address, IP address, bank details, medical information, and more.

Who will be affected?

The GDPR will apply to any organisation that handles any personal data of an EU citizen. This means that companies based outside the EU that provides goods and services to individuals living in the EU will need to comply with the new law.

When will it come into effect?

GDPR was approved and finalised in 2016. The new law will becomes effective on May 25th 2018

Why should I care now?

The countdown has already started. For some organisations, required changes to their IT security and data privacy program will be extensive. Organisations found to be in breach of GDPR risk significant fines.

How to Prepare

- Start by getting an understanding of what personal data is being held and who has access to it.
- Limit access based on business need and implement monitoring to detect any unauthorised access.
- Perform an assessment of what security controls you have in place to protect the data, how effective they are, and where the gaps are.
- Develop a plan to improve your security program, looking at people, process, and technology.
- Implement a personal data breach notification process, including incident detection & response capabilities.

Need help getting started?

Implementing the CIS Top 20 Critical Controls is a good place to start.

Download the quick guide
www.rapid7.com/7-steps