What You Need to Know About the

NEW EU DATA PROTECTION LAW

The proposed General Data Protection Regulation (GDPR) will regulate the privacy and handling of European Union (EU) residents' personal data. This will replace the existing EU Data Protection Directive, and unify data protection laws across the EU with a single set of rules.

Key Changes

While the GDPR is not yet final and the details are still being discussed and negotiated, we already have a good idea of major changes that are likely be included. 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 authorities and affected individuals without delay.
- **Penalties for non-compliance** – Fines up to 2% of a company's annual worldwide turnover or €1million, whichever is higher.

Common Questions

What is Personal Data?
Any information about an individual, whether it's to do with their private, professional or public life. This includes their name, photos, email address, IP address, bank details, medical information, and even social network posts.

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

When will it come into effect?
The current plan is for the GDPR to be finalised and approved by the European Parliament, the Council and the Commission by December 2015. Once approved, the new law will become effective across the EU after 2 years.

Why should I care now?
For some organisations, required changes to their IT security and data privacy program will be extensive. It's better to understand now what policy, process and system changes your organisation will need before the countdown starts.

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.
- Put in place a data breach notification process, including incident detection & response capabilities.

Need help on where to start?
Take a look at our Top 7 Security Controls Quick Guide under White Papers at www.rapid7.com