READY FOR THE EU GENERAL DATA PROTECTION REGULATION?

The EU General Data Protection Regulation (GDPR) has undergone more than 3,000 revisions since the EU Commission first proposed a single, harmonised privacy law for the EU in January 2012.

Key information

The latest updates suggest that the Regulation will be finalised by early 2016 and it is expected to take between one and two years to be enacted.

The EU GDPR affects:

- All companies in the EU
- Non-EU companies with data subjects in the EU

Heavy data breach penalties:

Up to 5% of turnover or €100 million - whichever is greater.

The aim of the GDPR is to:

- Improve data security for all.
- Create a unified, harmonised data protection law across the EU member states.
- Redefine 'personal data' to incorporate new personal identifiers such as biometric data.
- Implement a 'regulation' instead of a 'directive', which means that the same set of rules will be directly applicable to all EU member states without the need for state-level legislation.

"With data breaches continuing to dominate news headlines, organisations cannot afford to take a wait-and-see approach. Businesses must act now to ensure they are not caught off guard."

Alan Calder, founder and executive chairman of IT Governance

What are the key proposals?

Individuals:

- Will benefit from clearer, unambiguous data privacy policies.
- Must be informed about data breaches that affect them.
- Have the right to be forgotten.

Companies must:

- Seek explicit, unambiguous consent from individuals in order to process their personal data.
- Recognise that 'personal data' incorporates aspects such as biometric data.
- Incorporate privacy by design for high-risk projects.
- Conduct privacy impact assessments.
- Appoint a data protection officer.*
- Notify supervisory authorities in the case of a data breach.
- Prevent unauthorised access, use and disclosure of personal data (including copying, modification and erasure of data).

For instance, IT staff may not be allowed to view customers' personal data.

In the event of a breach, fines may be lower and there may be fewer data breach notification requirements if companies can prove that their data was encrypted.

Is your organisation prepared?

Find out how to prepare for the Regulation by taking our survey** now.

TAKE THE SURVEY NOW
http://www.surveymonkey.com/r/EURegSurvey

*Proposal relevant to companies with over 5,000 data subjects.

** All responses will be treated anonymously by IT Governance Ltd and not shared with third parties.