LogRhythm
The Security Intelligence Company

Are you preparing for the GDPR?

Get the facts and discover five actions you can take to prepare your business for the GDPR coming into force.

What is the GDPR?

The General Data Protection Regulation is intended to strengthen and unify data protection for all individuals within the European Union (EU).

Why is it coming?

The GDPR replaces the Data Protection Directive 95/46/EC, which was enacted before the rise of the internet and cloud computing. The GDPR will make compliance easier for businesses by providing a single set of EU-wide rules.

When is it coming?

The GDPR was adopted on 27 April 2016 and will be enforceable from 25 May 2018.

Who will it affect?

Anyone processing the personal data of EU citizens. In some ways, the GDPR is a global data protection law. Regardless of location, if you process EU personal data, you must comply.

Penalties

The consequences of not complying with the GDPR are formidable. Organisations can be fined up to €20m or 4% of global annual turnover, whichever is greater.

Fines from the Information Commissioners Office (ICO) against UK companies in 2016 would have skyrocketed from £880,500 to £69m if GDPR had been in force.[1]

4%
OF GLOBAL ANNUAL
TURNOVER

5 actions to take now to prepare for GDPR

01 Know your data.

What data do you hold? Where did it come from? Who is it shared with?

Action: Audit your data and update privacy policy notices for GDPR compliance.

02 Data subject access rights.

Be ready for data subjects exercising their rights: the right to access data, the right to be forgotten, the right to erasure and data portability.

Action: Update processes so requests can be responded to in time.

03 Data breach reporting.

Data breaches need to be reported within 72 hours of being detected. Are you able to detect and respond to a breach in that timeframe?

Action: Review your data breach reporting procedures.

04 Consent.

Do you have the required consent from personal data subjects to process their data? Guidelines on children's data are even more stringent.

Action: Review consent data and refresh existing consent to meet GDPR standards.

05 Data governance and compliance.

Secure engagement at all levels, determine whether you will need to appoint a data protection officer; privacy risk impact assessments will be required where privacy risks are high.

Action: Plan internal communications and training. Appoint data protection champions.

Gartner

Gartner predicts that by the end of 2018 more than 50% of organisations affected by the GDPR will not be in compliance with its requirements.[2]

50%
NON COMPLIANT

On average it takes organisations 87 days to detect a compromise. Nearly three full months.[3]

Faster detection and response is critical for complying with the GDPR. Talk to the LogRhythm experts to find out how Threat Lifecycle Managment can help you reduce the mean time to detect and mean time to respond to cyber threats and comply with GDPR.

LogRhythm
The Security Intelligence Company

Visit: www.logrhythm.com Contact: europe@logrhythm.com

[1]https://www.nccgroup.trust/uk/about-us/newsroom-and-events/press-releases/2017/april/last-years-ico-fines-would-soar-to-69-million-post-gdpr/
[2]http://www.gartner.com/newsroom/id/3701117
[3]https://logrhythm.com/pdfs/whitepapers/ir-security-intelligence-maturity-model-ciso-whitepaper.pdf