DATA SHEET

General Data Protection Regulation (GDPR)

LogRhythm
The Security Intelligence Company

What is it?

The General Data Protection Regulation (GDPR) will harmonize data protection laws in the EU and bring better transparency to help support individuals' rights and help grow the digital economy.

When is it coming?

The GDPR was adopted on April 27, 2016, and it will become law on May 25, 2018, following a transition period.

Scope

- The GDPR covers data processors (organizations) and data subjects (individuals) within the EU.
- Covers data export to other countries, including non-EU territories.
- GDPR applies to any organization processing the details of EU individuals.
- If you do business in the EU, you are subject to the GDPR.

Key Considerations for Security Professionals

1. Reporting data breaches

The GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" (Article 4, definition 12).

- Data breaches must be reported within 72 hours of being detected.
- Data processors are liable for any breaches.
- Penalties are determined at a maximum of $21 million or four percent of annual revenue—whichever is greater.

On the position of reporting the breach, the regulation states: "As soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it…" (Article 33).

2. Data protection by design

Under the GDPR, data protection and processing safeguards must become part of the DNA of all systems and processes.

Data protection by design is based on seven "foundational principles":

- Proactive not reactive; preventative not remedial
- Privacy as the 'default' setting
- Privacy embedded into design
- Full functionality: positive sum, not zero sum
- End-to-end security: full lifecycle protection
- Visibility and transparency: keep it open
- Respect for user privacy: keep it user-centric

Checklist: Reporting Data Breaches

The GDPR will require companies to develop or update internal breach notification procedures to meet the 72-hour reporting requirement:

- ✓ Timely detection of breaches
- ✓ Reporting and alarms
- ✓ Mitigation through automation
- ✓ Investigation capabilities (case management and forensics)

Checklist: Compliance and Data Protection by Design

The GDPR will require companies to rethink how data protection and privacy are met and managed by the organization:

- ✓ Analyze the gap between current and mandated position.
- ✓ Assign required budget and resources.
- ✓ Assign a data protection officer if criteria met.
- ✓ Align with best-practice mandates.
- ✓ Review and update data-handling procedures.
- ✓ Develop a workplace education program.

GDPR Language Defined

General Data Protection Regulation:

A regulation coming into effect in May 2018 to replace Data Protection Directive 95/46/ec and strengthen and harmonize the data protection rights of EU citizens.

Data protection directive 95/46/ec:

A 1995 directive on the protection of individuals which regulates the processing of personal data in the EU. To be replaced by the GDPR.

Personal data breach:

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Pseudonymization:

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.

Data protection officer:

A privacy expert who must operate independently to make sure an organization is following procedures and policies set out in the GDPR.

Data protection by design:

A key GDPR principle that states organizations will be subject to a specific obligation to include data protection considerations into a service, process or product from the outset.

Data controller:

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor:

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal data:

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly.

Learn more about the GDPR and how LogRhythm can help you comply to the upcoming mandate. Schedule your personal demo today.

logrhythm.com/schedule-online-demo/