Introduction to the New GDPR

This Executive Summary from CorreLog provides a brief overview of guidelines for maintaining GDPR compliance for mainframe and distributed systems with the best-practice Security Information and Event Management (SIEM).

> "The new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks. It's about moving away from seeing the law as a box ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organization."
>
> -Elizabeth Denham, UK Information Commissioner

The General Data Protection Regulation (GDPR) is designed to better protect and control European Union citizen's personal data. Effective May 25, 2018, it will bring some of the strictest legislation and compliance for data protection in the world. This new regulation will replace the Data Protection Directive (Directive 95/46/EC) and is designed to provide a single data protection law across the entirety of the EU, affecting organizations in all countries that have any contact with EU citizens.

No matter your location, if someone in your organization accesses identifiable data of a "subject," 16 years of age or older, who lives within the EU, as of May 25, 2018, your organization must comply with the regulation. Any data that could possibly identify a data subject must be audited and secured including name, photo, email address, bank details, social media post, medical information, or even computer IP address. Even for subjects who never become a customer, the organization must follow the GDPR.

This guide will provide a brief summary for executives of CorreLog's in-depth rubric of the EU's 88-page GDPR from the CorreLog whitepaper titled, *"Impact from the New GDPR: The Countdown to May 2018 has Begun."* Learn the best ways to prepare your organization, including how to manage your weakest threat vector and the importance of having a security system that provides report breaches in real-time, as well as, the top points that need to be on your radar as we get closer to May 25.

What to Watch for with the GDPR Compliance

Data File Types

The GDPR applies to any organization that "offers goods or services to, or monitor the behavior of EU data subjects", regardless of the company's location.

Appointing a DPO

If your organization falls into the category of public authorities, organizations that engage in large-scale systematic monitoring, or engage in large-scale processing of sensitive personal data, you may be required to appoint a Data Protection Officer.

Processing Child Data

Parental consent is required to process personal data of children under the age of 16. Member states have the option to reduce this age limit but not below 13 years old.

Data Breach Reporting Time-frame

Organizations must notify a supervisory authority competent no later than 72 hours after having become aware of a breach.

Processing Activity for Goods and Services

The regulation applies to all organizations that offer goods and/or services to EU residents whether a payment is transacted or not. If you market your goods/services to any EU citizen or organization, the GDPR applies to both customers and prospects in your contacts list.

Subjects' Legal Right to be Forgotten

Citizens under the protection of the GDPR have the "right to obtain from the controller the erasure of personal data concerning him/her without undue delay". Organizations must have a method for data subjects to request erasure.

Transfer of Personal Data to Third-party Countries

The regulation acknowledges that the transfer of data is normal for conducting international trade but states "all provisions…shall be applied to ensure that the level of protection is not undermined."

Non-Compliance Penalties

Not following the regulations of the GDPR can result in fines up to four percent of global annual revenue or €20 million, whichever is greater. The lower level penalty is set at two percent of revenue or €10 million.

5 Things to Help Prepare for GDPR

1. *Have Security Information and Event Management (SIEM) visibility and correlation from all sources*

   To keep tabs on your data, you need a 360-degree view of all user activity surrounding your data. Collecting event logs from mainframes, endpoint devices, firewalls, routers/switches, desktops, servers, and applications (log management), and then correlating them against norms of user behavior (events) are the basics of SIEM that will help with the GDPR.

2. *Reinforce your endpoint threat vectors*

   Mobile devices might be the most vulnerable threat to GDPR. Your enterprise mobility management (EMM) system is a great tool for provisioning and managing devices, but it was never designed to be enterprise security. Event logging and event correlation must be combined into a single view of data security within your SIEM or IT security operations center (SOC).

3. *Real-time alerting system*

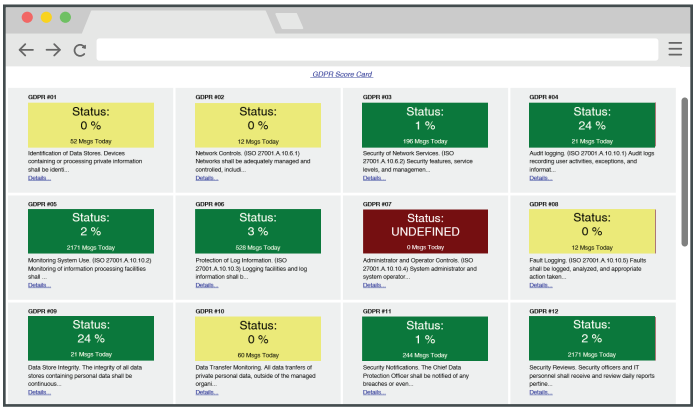
   With the GDPR's 72-hour breach alert deadline, you need a real-time alerting system across all threat vectors and alert messages sent to a SIEM system or SOC. Your mainframe must include real-time event messages sent to a SIEM system or SOC when anomalous behavior is detected.

4. *Having an alerting system that can trigger your enterprise Service Desk assists with the 72-hour rule*

   Your EMM and SIEM processes need to have the capability to issue a trigger to a notification system that a potential breach needs to be investigated. In addition, an automated email or SMS text should be generated to security admins.

5. *Get your legal team involved now*

   The GDPR represents some of the most stringent data protection laws in the world. With the EU's 30-member states, each state can regulate the GDPR differently and the hefty fines and vague language should be enough to make your legal team take a serious look at the legislation.



CorreLog's GDPR scorecard provides a one-window view of important GDPR metrics and most importantly, the health of your GDPR compliance.

CorreLog's Approach to GDPR

CorreLog's mainframe SIEM products are designed to deliver real-time notifications from z/OS, Db2, IMS, Linux on z, Windows, UNIX, Linux, SAP, and other open-source systems to any SIEM or Security Operation Center. CorreLog can be a valuable resource for a single repository of event log data across all systems, mainframe and distributed, with the visibility to stay out in front of any trouble the GDPR may bring. CorreLog products have the ability to see anomalous behavior as it occurs in real-time and the ability to alert appropriate security personnel if a threat does happen.

In Summary

This executive summary is an introduction to CorreLog's more detailed whitepaper, titled *"Impact from the New GDPR: The Countdown to May 2018 has Begun,"* written to help companies understand the policies and origin of the GDPR, how to prepare for it, and the functionality within CorreLog's mainframe SIEM tools that can help maintain your GDPR compliance.

Visit CorreLog.com/library to download the GDPR compliance whitepaper and other CorreLog security, compliance, and auditing documents.

CORRELOG®
CorreLog.com

CorreLog, Inc.
1-877-267-7356 Toll-free (US only)
+1-239-514-3331 International
info@CorreLog.com