WHAT GDPR MEANS FOR LOG MANAGEMENT

In April 2016, the European Parliament adopted the General Data Protection Regulation (GDPR), which requires businesses to protect EU citizens' personal data and privacy regarding transactions within all 28 member states and regulate personal data exportation outside of the EU. Companies must demonstrate compliance by May 25, 2018.

The GDPR replaces 1995's data protection directive. That directive fails to address how data has come to be stored, gathered, and transferred. The GDPR seeks to address data security shortcomings by aligning regulators under a single authority and asserting updated privacy rights for more than 500 million EU citizens.

WHY DOES GDPR EXIST?

The previous data protection directive passed long before the Internet became the primary marketplace for businesses. In light of recent data and privacy issues, consumers demand higher standards for more security.

WHY SHOULD COMPANIES CARE?

Before GDPR, Big Data was an asset. Now, it could be perceived as a liability. Broadly speaking, the less customer information an organization stores, the lower their risk. Companies across the EU and U.S. expect GDPR to set new standards for consumer rights and data security. Such changes inevitably lead to a number of challenges—GDPR standards are high, requiring large investments in achieving and maintaining compliance.

One new standard: companies must provide a reasonable level of protection for personal data.

22% OF COMPANIES UNAWARE THEY MUST COMPLY WITH GDPR

Solix Technologies

PERSONAL DATA IN LOGS

Under GDPR, access logs, error logs, and security audit logs will now be considered to hold personal information. Companies must protect IP and cookie data as they would personal identifiers. Additionally, personal data cannot be collected or stored without documentation of individual consent. However, personal data can be collected and stored with web server logs to help detect and prevent fraud or unauthorized system access.

WHY IS GDPR IMPORTANT RIGHT NOW?

Consumers value their privacy and data security more than ever. According to the RSA Data Privacy & Security Report, consumers are changing their behavior to protect themselves, often to the detriment of data-reliant businesses. More than 40% of RSA report respondents claimed they falsify data when registering for online services. Half of respondents said they would favor companies that protect data, and more than 70% would boycott companies that seem to not. Companies who don't take GDPR compliance seriously won't just face stiff financial penalties but could also face trouble with customers.

52% OF COMPANIES BELIEVE THEY WILL FACE NON-COMPLIANCE FINES

Ovum

CORE AREAS FOR GDPR READINESS

While GDPR affects several areas of business, there are a few key areas companies can strengthen to help achieve compliance.

TRANSPARENCY

Companies will need to provide clearer communication on personal data use and mandatory breach disclosure. They'll face tougher consent rules and have to work with stronger data subject rights. For instance, companies must:

- Inform subjects of what data processing will be done. Processed data must match how it has been described to the subjects.
- Report breaches within 72 hours of detection to supervisory authorities and affected individuals.
- Perform impact assessments to help mitigate risk of breaches.

COMPLIANCE

Although there are exceptions, GDPR doesn't supersede legal requirements that organizations maintain certain data—for instance, HIPAA requirements for health records. Still, among other controls, companies should be particularly mindful of the following:

- Privacy by design and default
- Data protection impact assessments
- Documented data use
- Data portability and personal data erasure upon request (right to be forgotten)
- Enhanced rights of inspection and audit for supervisory authorities

ACCOUNTABILITY

Adhering to GDPR will be necessary to maintain customer relationships and to avoid punishments, though it remains unclear how these punishments would be assessed. The following are just some of the consequences fo GDPR non-compliance:

- For technical measures: financial penalties up to €10 million or 2% global annual turnover, whichever is higher
- For key provisions: financial penalties up to €20 million or 4% global annual turnover, whichever is higher
- Supsension of the right or ability to process data

GDPR COMPLIANCE PRINCIPLES

There are numerous areas in which GDPR demands compliance, but overall, companies can focus on these principles to help them become compliant.

BE FAIR

Process personal data lawfully and transparently by informing consumers what data processing will take place, and ensure that the description matches the process.

HAVE A REASON

GDPR states that personal data should be obtained only for “specified, explicit and legitimate purposes.” Companies must also inform consumers of those purposes.

MINIMIZE DATA

Keep only personal data that is adequate, relevant, and limited to what is necessary in relation to processing purposes.

STAY UPDATED

Personal data must be up to date and accurate. Archiving activities for consumer data requires rectification processes.

KEEP ONLY AS LONG AS NECESSARY

Remove data no longer required, obtain consent to store and process data, and ensure data is portable.

PROCESS APPROPRIATELY

To prevent loss, damage, or destruction of personal data, it must be processed in an appropriate manner.

WHO DOES GDPR AFFECT AND HOW?

GDPR defines several roles responsible for compliance, and places equal liability on organizations that own data and those who help manage it. Companies with processor partner contracts should clarify responsibility and data management processes to help with GDPR.

38% OF COMPANIES WITH PERSONAL DATA UNPROTECTED AT EVERY STAGE OF ITS LIFE CYCLE

Solix Technologies

DATA CONTROLLER

This role defines how to process personal data and why. The controller also takes responsibility for ensuring third-party processors comply with GDPR. If third-party processors do not meet GDPR compliance, the primary organization is also considered non-compliant.

DATA PROCESSOR

Data processors could comprise outsourcing firms or internal teams that maintain or process personal data records in any way. Both a company and processing partner would be accountable for breaches or non-compliance.

DATA PROTECTION OFFICER (DPO)

Under GDPR, companies must have a DPO if they are a public authority or handle large amounts of data gathered from EU citizens. Controllers and processors must assign a DPO to oversee compliance and data security strategy, though law enforcement agencies could be exempt from such DPO requirements.

HOW GRAYLOG HELPS WITH GDPR COMPLIANCE

Complying with GDPR requirements involves proper planning for how your organization handles data and then protecting that data. The data in your logs provide useful records of information about your customers, users, applications, servers, networks, devices, and activity across your IT environment.

You can deploy Graylog to meet several GDPR requirements related to how your organization handles personal data.

DATA PLANNING

When getting ready for GDPR compliance, you must evaluate how you currently control and process personal data to ensure those policies and processes fit within the new requirements. While this is a necessary step at the initiation of GDPR compliance, you should document these policies, integrate them into your information security processes, and review them at regular intervals.

DATA FLOW PLANNING

Mapping how your data flows throughout your network is the first step in GDPR compliance. It's essential to understand where the personal data relevant to GDPR is located. If you are not already storing your data in a central repository, it makes sense to import all of that data into Graylog, where its powerful search can quickly identify reports or applications that rely on personal data.

PERSONAL DATA RETENTION POLICY

GDPR specifies limited retention of personal data and under the regulation, organizations are required to delete the data when it is no longer needed or deletion is specifically requested from a data subject.

Graylog lets you:

- Set data retention policies quickly and easily from within the user interface
- Establish policies without additional components or tools
- Define different retention periods for different types of data, allowing you to change personal data retention periods without affecting other types of data you might collect

DATA PROTECTION

Once you have planned the flows for the personal data in your environment, it's time to put the appropriate level of protection in place for those data flows. The GDPR requirements surrounding data protection focus on the security of personal data when processing.

Graylog not only serves a secure datastore for personal data to meet these requirements, it also acts as a centralized security logging and analytics platform when handling data inside Graylog or in other data platforms. You can deploy Graylog on a secure system to meet the following GDPR requirements.

DATA PROTECTION BY DESIGN

Using Graylog as your datastore for personal data helps with GDPR compliance right from the start from within the Graylog user interface:

- Treat data as a valuable asset by limiting access
- Ensure data is secure
- Maintain accuracy
- Limit retention
- Minimize personal data
- Separate data by project

These capabilities are included in the Graylog product for free.

ENCRYPTION AND PSEUDONYMIZATION

To properly secure personal data, multiple levels of protection are required to ensure data is not lost, destroyed, or disclosed to unauthorized individuals. Graylog supports deployment on systems that use disk-based encryption. This kind of encryption greatly decreases the possibility of unauthorized individuals accessing personal data in clear text.

GDPR also calls for pseudonymization of personal data, which is defined as "…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." The Graylog processing pipeline functionality allows flexible pseudonymization or any kind of data, or even parts of data.

ACCESS CONTROLS

To prevent unauthorized access to personal data, there must be some way to authenticate users. Graylog includes common access control capabilities such as integration with external authentication sources such as Active Directory or LDAP and password protection.

GDPR not only requires authenticating users but also verifying that the roles to which those users are assigned are appropriate for the data they can access and the tasks they can perform. You can manage all of these access control capabilities through the Graylog interface without the need for additional components or logic.

LOGGING AND AUDITING

GDPR compliance requires you to store personal data in logs and have the ability to audit the data in those logs. Using Graylog Enterprise as a datastore for your personal data enables you to maintain an audit log for security events to see who is accessing what and what they're doing.

If Graylog is not the primary datastore for your personal data, you can still use Graylog as a centralized platform to manage logs from throughout your infrastructure that could contain personal data. Either approach gleans valuable insight into the security of the personal data you store.

MONITORING AND DETECTION

Monitoring personal data includes monitoring datastore health, log continuity, and detection of malicious activity within your environment. Graylog makes APIs available for integration with other monitoring tools. Also, Graylog uses a message journal to ensure your data is always delivered in case of an interruption or failure. Graylog Enterprise keeps a detailed audit log so update and delete actions on indices can be monitored. Graylog Enterprise is designed to enable threat hunting, even internally, rather than being another black box on the network.

RESILIENCE AND RECOVERY

Purpose-built for log collection, management, and analysis, Graylog scales easily to continue operating smoothly during times of high volumes of events. Additionally, its archiving mechanism stores logs in optionally encrypted files for easy movement to secure locations, allowing for convenient and simple backups.

MAINTENANCE OF DATA SUBJECT RIGHTS

When a data subject requests deletion of their personal data, or no longer allows their personal data to be collected, you must be able to easily find that data throughout your infrastructure to fulfill their request. Graylog search capabilities enable you to quickly find all queries, reports, and tables that might contain that personal data. Since Graylog stores archived data in plain text files, it's simple to delete that personal data in the archives with standard tools, rather than requiring additional APIs or plugins to fulfill this GDPR requirement.

CONCLUSION

The GDPR compliance deadline has arrived, and it's a long-term and ongoing process to implement controls and policies that continue to meet the regulation's requirements. Becoming GDPR-compliant will likely be an expensive and time-intensive task for many organizations.

Graylog technology can speed up the process and ensure your data management processes and policies are ready for the future. Using Graylog as your primary datastore gives you security, access control, monitoring, resilience, auditing, and recovery capabilities, most of which are controlled directly through the user interface. Additionally, the auditing and archiving capabilities of Graylog Enterprise help your organization further align with GDPR principles surrounding data protection, personal data minimization, and data subject rights.

www.graylog.com
support@graylog.com
708 Main Street, Houston, TX 77002