LOGmanager and compliance with GDPR

A white paper illustrating how deploying LOGmanager helps ensure compliance with the requirements of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (GDPR).

The GDPR lays down binding rules on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

In 2012, the European Commission proposed a thorough revision of Directive 95/46/EC (General Data Protection Regulation). This became the basis of a new regulation generally known as the General Data Protection Regulation (hereinafter "GDPR"), approved in April 2016. The GDPR has been designed to harmonize the so far different laws on personal data protection and processing across all EU Member States. It will come in force on 25 May 2018 and will apply to all organizations processing personal data of EU citizens, both inside and outside the European Union. The key requirements of the GDPR include in particular the following:

- Strengthen the protection EU citizens with regard to the processing of their personal data.
- Incorporate the requirements concerning the safety of data and own systems into the process of development and deployment of the software used for personal data processing (privacy by design and by default).
- Protect personal data to the maximum extent possible by using anonymization, pseudonymization and encryption.
- Protect personal data, their availability, confidentiality, and the actual personal data processing.
- Create new organizational roles and processes to reinforce supervision over the safety of personal data.
- Regularly test, assess and evaluate the effectiveness of technical and organizational measures for ensuring security of processing operations.
- An obligation to notify the relevant supervisory authority no later than 72 hours after becoming aware of a breach of the GDPR or of a loss of personal data.

In order to support the enforcement of the Directive, GDPR includes also a provision on penalties including administrative fines, which can reach astronomical sums. Unfortunately, the Regulation (EU) 2016/679 of the European Parliament and of the Council stipulates that these sanctions must be applied to a maximum extent, with the possibility to use alternative measures only in the case of natural persons.

Because the Regulation is written in a technical language that is sometimes difficult to understand, many organizations ponder what measures and in what areas are they obliged to comply with according to GDPR requirements. They also ponder what systems and solutions might reliably ensure compliance with GDPR requirements.
This document describes how compliance with some key requirements of this legal norm can be achieved by introducing appropriate system of centralized collection and management of security events built on the LOGmanager platform.

Executive summary for CISOs/CIOs:
GDPR and LOGmanager

LOGmanager and its relation to GDPR: In brief, LOGmanager allows organizations to perform ongoing as well as one-off audits and clearly document any identified personal data breaches including **who, when and how accessed the data and systems that are subject to GDPR**.

LOGmanager is a certified platform for management of audit records according to ISO/27001:2013. In an encrypted* repository, it retains event logs on a long-term basis in a managed, centralized, indexed and compressed database. The event logs are converted to a normalized format to allow convenient use, but they are also stored in their original form. All records carry a unique identifier and are protected by a trusted timestamp. The verification and authorization mechanisms used by LOGmanager as well as its in-built control mechanisms ensure that the stored data can be accessed by authorized persons only and there is no known way how to modify or partially delete the data.

** Encryption is available only for LOGmanager running on HPE servers using HPE Secure Encryption.*

However, the implementation of an audit is an important part in the overall chain of measures, it is necessary to point out that this is only one step in many. On the other hand, not even the implementation of all technical and organizational measures as stipulated by the Regulation releases a company from its liability for a failure to comply with the objectives of the Regulation. (*Yes, a legal norm designed as described can have some potentially alarming consequences. There is no need to anticipate or suggest any catastrophic scenarios. Only future court decisions regarding cases of GDPR breach will show what is the application of the GDPR provisions in practice.*)

Detailed information for IT security professionals in organizations

In what specific GDPR-related areas can LOGmanager be useful.

Article 32 – Security of processing
Article 33 – Notification of a personal data breach to the supervisory authority
Article 34 – Communication of a personal data breach to the data subject
Article 58 – Powers

Monitoring of the security data processing and access to personal data:
LOGmanager has been developed as a centralized management system for event logs that provide a simple view of all machine-generated data in an organization. In the first step, LOGmanager collects, unifies and ensures long-term storage of logs and events obtained from active network elements, security devices, operating systems and application software Subsequently, in near real time, it saves the collected data into a well-defined high-performance database that can be accessed by IT security specialists via a set of predefined dashboards or structured and full-text queries with graphical representation of results.

Superior traceability of logs, events, and other machine data can be used, besides, also to implement measures required by the GDPR. In addition. Moreover, LOGmanager provides a powerful application interface supporting integration with other tools used by the organization for both monitoring and security purposes.

To comply with the above-described requirements, LOGmanager provides log management mechanisms and guarantees the ability to trace back system and user-generated events and perform their ongoing or one-off audits. This is critically important for preventing, detecting, or minimizing the impacts of compromising data or systems that are subject to GDPR. As LOGmanager provides a single pane views of all machine data, it is possible to trigger detailed tracking, alerting, and analysis when a security issue is detected. Briefly, it is an all-in-one application for log collection, storage and analysis that enables cost-effective automation of security measures and proactive protection of IT systems and networks.

LOGmanager is a tool enabling implementation of some of the measures prescribed by the GDPR. Nevertheless, it provides also tools to manage cyber-attacks and cyber-security incidents. For IT security specialists, it provides controlling and auditing tools. In an unambiguous and indisputable way, it records the operation of the systems allowing detection, collection and evaluation of security events, and can continuously monitor the availability of information from the machine data obtained.

The obligation to report incidents and cooperate with the supervisory authority:
LOGmanager allows to create documents in the required format as necessary for reporting security incidents and it enables organizations to document the security of their systems that are subject to GDPR. Thanks to sufficient retention of the stored machine data, it allows to create audit records and prepare documents that are required for the reporting of and subsequent forensic analysis of the detected security events, even if the time of the occurrence of a security incident and the time of its detection differ significantly*.
** Data retention capability is dependent on LOGmanager version and on the volume and type of the collected machine data. The XL LOGmanager model, which uses a 100 TB database and collects 3,500 events per second, achieves the average data retention of 450 days. According to recommendations by National Center for Cyber Security all LOGmanager versions comply with the relevant data retention and integrity control requirements, log encryption requirements, as well as requirements concerning encrypted transfer of logs into the log management system.*

LOGmanager

LOGmanager allows to generate, in a well-defined table format, operational data (machine data) and data generated in connection with activities that are subject to regulation.

LOGmanager and the collection and processing of PI - FAQ:

Is it necessary to have a consent of the subjects, while processing their PI data in LOGmanager?

No additional consent is required. If a person has agreed to process his/her personal data in your organization, it is highly probable that some of its personal information will appear in security, surveillance, audit or forensics. Amid personal data that may appear in LOGmanager are most commonly the name, username, IP address, and e-mail address. As for LOGmanager, it is a system, where the purpose of collection and processing is defined as **Lawful basis for PI data processing.**

LOGmanager processes logs, events, security, and system data solely for security, audit, and forensic analysis. The very security and audit reasons are a legitimate interest. Nevertheless, we strongly suggest that company data protection officer should create some paperwork around LOGmanager.

Using the Internal Guidelines for Personal Data Management, please create a document that will:

a) **Define the purpose of the collection** – in this case, it is security, audit and forensic analysis platform to investigate security incidents and prevent loss or violation of the integrity of personal data.
b) **Document the wherewithal used for processing** – LOGmanager is a collector and central log storage, which can also contain selected personal data from the audit of systems processing personal data from sources that provide the events, logs, and machine data.
c) **Perform the warranty documentation, access restrictions and security measures to protect potential personal data stored in LOGmanager** – describe how your AAA LOGmanager setting is addressed, who is a member of the team, who can perform a LOGmanager operation and what database permissions has regarding to personal data.
d) **Make documentation, how the historical data from LOGmanager is deleted** – adduce that data in LOGmanager cannot be modified in any way. When the database storage space is full, the historical data is automatically deleted by the retention policy of the LOGmanager. If you back up your LOGmanager data to external systems, you must also indicate how data backups are stored and protected from unauthorized access. In addition, it is necessary to indicate how the backups, which are no longer needed for the above purposes, are deleted.
e) Define and document regular control measures related to LOGmanager.

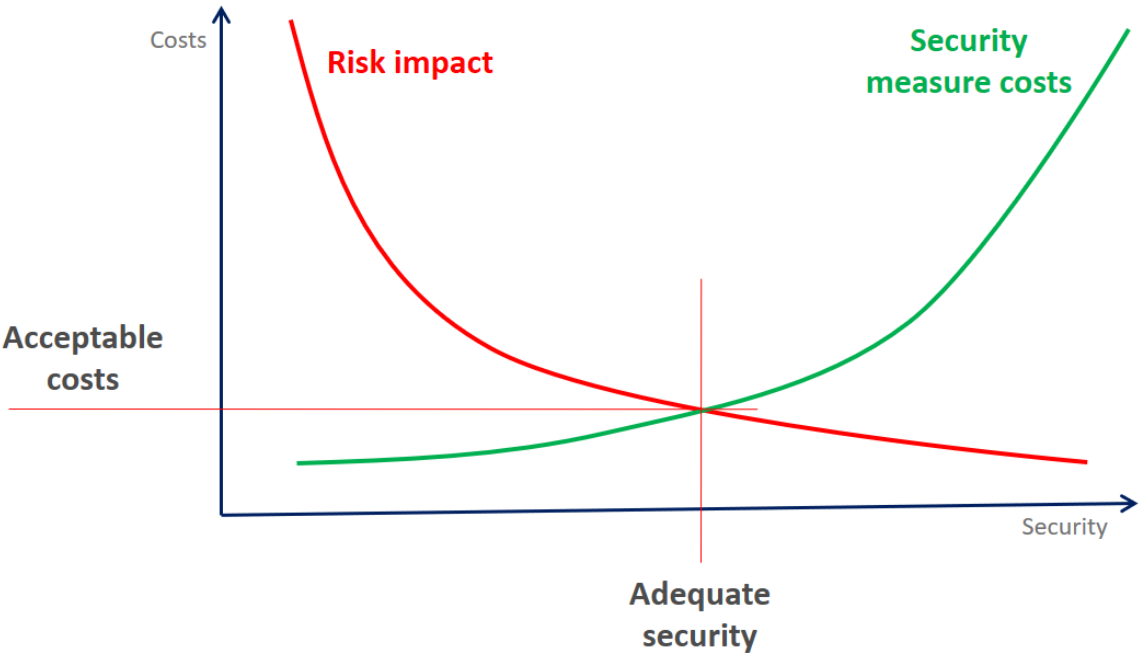
If the entity revokes consent, is it also necessary to delete its personal data from LOGmanager?

It is not. The processing of audit logs in LOGmanager is a legitimate interest of the personal data processor. Even after the withdrawal of the consent by the subject, it is necessary to keep the audit data generated. Documentation of previous processing activities and possible evidence of deletion from production systems is the main reason, why to do not delete the data.

LOGmanager

LOGmanager – the right choice to ensure GDPR compliance

Before implementing measures according to regulatory requirements, it is necessary to perform risk analysis and evaluate the total costs of individual solution options while ensuring maximum compliance with regulations. And, of course, overall efficiency of given solution for organization.



LOGmanager offers the following key benefits to organizations seeking an optimum balance between the level of security and reasonable costs:

- Fast on track. Implementation ensuring regulatory compliance is a matter of days.
- Easy staff training in 2 days to full skillset.
- Friendly and intuitive multi-language user interface.
- Detailed documentation in English plus instructions on how to appropriately set up event sources.
- LOGmanager user forum with additional tech tips and hints.
- Low, and mainly well-defined operating costs. Hardware, software and services are included in the price.
- No hidden licensing costs. LOGmanager does not carry any license restrictions.
- Full compliance with ISO/IEC 27001:2013, compliance with EU country specific regulatory requirements.