Technical and organizational measures for the protection of information and PII

Directive

File Name:
M3D_3503_sl_global_en_Technical_and_organizational_measures_for_the_protection_of_information_and_PII,
23 January 2025

Table of Contents

Scope

This directive applies to all companies within the Swisslog Business Segment as part of the KUKA Group. These companies are henceforth referred to in this document as Swisslog.

Purpose

The appropriate and risk-oriented protection of sensitive information, regardless of whether it is internal information, information from third parties (customers, business partners, etc.) or personally identifiable information, is a high priority for Swisslog. This document underlines Swisslog`s commitment to adequately protect the confidentiality, integrity and availability of critical infrastructure, systems, applications and (personally identifiable) information to ensure a high level of Information Security and Data Protection, both within Swisslog and the Supply Chain. To ensure an adequate level of protection throughout the supply chain, the measures listed below define the minimum level of protection that Swisslog`s suppliers and business partners must ensure.

The following list of technical and organizational measures are also prescribed by Article 32 of the European General Data Protection Regulation (EU-GDPR) to ensure the security of the processing of personally identifiable information. Pursuant to Article 32 EU-GDPR, data controllers and processors are obliged to take appropriate technical and organizational measures to ensure a level of protection appropriate to the risk. The state of the art, the costs of implementation and the nature, scope and purposes of the processing are to be taken into consideration when determining the measures. Pursuant to Article 24 Para. 1 and Article 32 Para. 1, there is an additional obligation for regular review and, if necessary, updating of the document.

1. Confidentiality

1.1 Physical access control

In general, the organization`s premises and buldings are divided into different security zones depending on the protection needs of individual departments and areas. State-of-the-art RFID transponders with individual access authorizations are used at the entrances and throughout the rest of the buildings. Visitors are recorded throughout by a central visitor process. Due to the transponder systems used, access to secured areas is only possible if accompanied by an authorized employee.

Unauthorized access to information processing systems with which information are processed or used is prevented by means of various technical and organizational measures. Measures include securing the building with an alarm system, monitoring access using installed video surveillance systems, conducting visual inspections by security personnel, cards or keys and other physical entry controls.

Service rooms and offices in which confidential data are processed (including management, personnel office, etc.) are always locked in the event of absence, even during business hours. It is ensured that all measures for the protection of information and personal data are also complied with in the case of employees working from home.

1.2 System access control

Within the company, it is ensured that only authorized employees or supervisors have access to applications, systems and information based on the principles of Need-to-Know and Least Privilege. From a technical point of view, individual identification is ensured for each employee by means of a username and password. Passwords are of a complexity that corresponds to the state of the art. Initial password changes and compliance with complexity is enforced using technical measures. Additionally, other security technologies, such as multi-factor authentication or continous authentication (e.g., SSO), are used.

Data storage media in notebooks and desktop computers are secured against unauthorized access by hard-ware-level encryption.

Whenever the workplace is left temporarily, computers must always be locked by activating the password-protected screen saver. From a technical perspective, the computer is locked automatically after a reasonable period.

Client systems are protected against viruses, trojans and other attacks by protection software from a renowned manufacturer. The required signature updates are carried out at appropriate intervals. Additionally, central patch management ensures that client systems are always supplied with the latest security updates.

The company network is protected from external and internal attacks using firewalls and malware scanners. The critical IT infrastructure is located in ISO/IEC 27001 certified data centers. External access to IT systems is only possible in a controlled manner and exclusively via encrypted connections.

In addition to technical measures, access control is reinforced by organizational regulations. These include internal company guidelines on data protection and information security, such as the secure handling of mobile data storage media. Employees are required to comply with existing policies.

1.3 Data access control

The company takes state-of-the-art measures to control access to data processing equipment and IT systems. The measures implemented pursue the objective of ensuring sufficient protection against unauthorized reading, modification, or deletion of data by unauthorized persons.

From a technical perspective, the document shredders distributed throughout the building protect documents that are no longer needed against unauthorized access. Additionally, document shredding containers are used, which are collected at regular intervals by a certified service provider and disposed of in accordance with ISO/IEC 21964 in a data protection-compliant manner.

As a general rule, all data storage media are erased by means of an appropriate process before further use or decommissioning and are also mechanically destroyed if necessary.

From an organizational perspective, all information is classified according to its protection needs and an individual and documented rights and roles concept exists for all IT systems and applications. This enables differentiated control of access to data. The assigned authorizations are reviewed regularly and adjusted as required. In particular, in the event of hiring, internal company changes or termination of the employment relationship, the authorizations are changed immediately. The assignment, modification and withdrawal of authorizations are documented.

Access authorizations are managed exclusively by authorized administrators. Administrator accounts are kept to a minimum and are only available to a select group of people. Access to confidential information and personal data is regulated in such a way that employees only have access to data that are required for the performance of their respective tasks.

1.4 Separation control

The company employs separation control measures to ensure that the data processing is always carried out in accordance with its actual purpose. Appropriate techniques are used to ensure that information of customers, clients, and the company itself are processed in such a way that they are separated logically or physically. Multi-client capability is considered for relevant applications. Production and test systems are separated from each another. From an organizational point of view, separation control is achieved by means of authorization concepts and the definition of database rights.

2. Integrity

2.1 Transfer control

Transfer control measures ensure that information is protected from unauthorized modification, but also from unauthorized reading or copying. To ensure this, only encrypted connections in the form of VPN or SSL technologies are used for data transmission.

If required, confidential information – insofar as such information is forwarded on external data storage media – are secured by means of adequate cryptographic procedures. Where possible, personal data are pseudonymized or anonymized.

Before data storage media that are no longer required are passed on, they are either securely erased or destroyed in accordance with the state-of-the-art and relevant data protection regulations.

2.2 Entry control

Measures for entry control pursue the objective of being able to guarantee the traceability of inputs, changes, or deletions of data. This is ensured by organizational measures in which individual usernames are used instead of user groups. Only authorized employees have the possibility of making changes to information and personal data, depending on their function and activity. Additionally, clear responsibilities are defined for deletions within the company.

3. Availability and resilience

3.1 Availability control

The company takes state-of-the-art measures to ensure the continuous availability and resilience of information, applications and systems. The objective of the measures implemented is to ensure permanent protection against data loss, incidents or other damaging events.

To achieve this objective, IT Desaster Recovery, Business Continuity and Back-Up concepts are available. Among other things, this ensures that all relevant server systems are connected to uninterruptible power supplies (UPS) and that sufficient redundancies are in place as fail-safe measures.

Additionally, the systems are integrated into a comprehensive system and network monitoring system so that it is possible to respond promptly to failures in the event of a malfunction. From an organizational point of view, a proven backup & recovery concept is in place so that it is possible to restore operationally critical IT systems and data in the shortest possible time. Backup operations are controlled and logged. External backup media are always encrypted. Additionally, recovery tests for

data recovery are carried out at regular intervals. The data center is audited at regular intervals so that the correct implementation of the measures adopted can be verified.

4. Incident Management

4.1 Incident preparation and handling

Clear roles, responsibilities and processes are defined in relation to incidents in the area of Information Security and Data Protection. This includes, among other things, reporting channels for incidents, classification of incidents depending on their criticality, escalation mechanisms and centralized documentation. Depending on the type and extent of the incidents, lessons learned exercises are carried out. Furthermore, there are corresponding emergency concepts and incident handbooks that are used as playbooks. The processes and concepts are regularly tested in simulated crisis exercises.

4.2 Supplier reporting obligations

Suppliers shall be obliged to protect the information used for the provision of the deliverables, including personal data, provided by Swisslog, against unauthorized access, modification, destruction, and other misuse ("Information Security") using state of the art technology. Suppliers must inform Swisslog of any suspicion of a violation of the requirements of

- export control,
- data protection and
- information security within 24 hours from the time of discovery

and must provide Swisslog with all information required to clarify the facts of the case via infosec@swisslog.com and to restore the original position before such violation quickest possible.

Swisslog has the right, in consultation with the Supplier, to carry out inspections regarding the above-mentioned violations or to have them carried out by examiners to be appointed in individual cases. Swisslog has the right to satisfy itself of the Supplier's compliance with the requirements in its business operations by carrying out spot checks, which in general shall be announced in advance.

The Supplier is obligated to immediately notify Swisslog in writing of not only insignificant compliance violations, but also for specific violations that may directly or indirectly impair the Supplier's willingness/ability to perform and/or the business relationship of the parties. In the event there is suspicion of inadequate quality of the deliverable and justified cause (for example in the event of non-compliance with agreements, milestones, etc. by the Supplier), Swisslog shall have the right to inspect the performance of the deliverable with the Supplier during normal business hours and to inspect the materials, documents and performance results directly or indirectly related to the deliverable.

5. Regular review

5.1 Data protection management

To meet the requirements of the European General Data Protection Regulation, various organizational data protection management processes have been established within the organization. These pursue the objective of ensuring continuous implementation of data protection in the company. The company enters the established processes, tasks, and documentation in a data protection management system (DPMS).

An internal Data Protection Officer has been appointed for the company. He/she advises and informs data controllers, data subjects or processors on data protection issues. He/she monitors compliance with the requirements of the GDPR and the internal data protection agreements and cooperates with the competent supervisory authority. If required, data protection impact assessments are carried out for required processes or technologies. The data protection officer uses his/her expertise to provides support here.

The company complies with the information obligations pursuant to Art. 13 / 14 GDPR. All employees are bound to confidentiality by a written agreement and made aware of this. Adopted policies and technical measures are designed to ensure that employees working from home also comply with them.

The internally appointed Chief Information Security Officer (CISO) additionally develops measures and guidelines to ensure that desired IT security strategies are implemented effectively. All employees are given practical training related to Information Security and Data Protection at regular intervals

5.2 Control of external processing

If third parties are commissioned with the processing of personal data, suitable measures are taken to ensure that data are only processed in accordance with the client's instructions. All contractors are selected with due diligence regarding data protection and information security to ensure a protection level which at least equals the measures described in this document. Necessary external processing agreements are always concluded with all contractors. The existing contracts for external processing are regularly checked by the Data Protection Officer for correctness of content.

6. Updating of measures

The technical and organizational measures are reviewed at least once a year to ensure that they are up to date, appropriate and adapted if necessary. If there are significant changes to the implemented measures outside of the review cycle, the documentation of the technical and organizational measures is adapted directly. In every review of the measures used, care is taken to ensure that measures are designed using state-of-the-art technology and information security as well as data protection-friendly default settings.