KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

# Technical and Organizational Security Measures at Krones (TOMs)

# Part A - General technical and organizational security measures at KRONES (GTOMs)

## Description of technical and organizational policies and procedures implemented in conformance with article 32 GDPR

For the protection of personal data Krones AG has implemented a comprehensive set of technical and organizational measures and continuously improves them. This part gives an overview over general measures that are applicable to basic processings used in all of our digital services. For specific digital products or services specific technical and organization security measures ("STOMs") may complement these general measures.

Krones has established a group-wide Information Security Management System (ISMS) and Data Protection Management System (DPMS). ISO/IEC 27001 is used as a guiding principle for the ISMS. Krones has appointed a Corporate Information Security Officer and a Data Protection Officer. Data protection and information security training is provided to employees on a regular basis. All employees who come into contact with personal data have committed themselves to confidentiality and data secrecy according to the provisions of art. 28 sec. 3 p. 2 lit. b, 29, 32 sec. 4 GDPR.

The internal IT-Services provided by the Information Management at Krones AG are the basis for our development, maintenance and operations activities. Krones Information Management is ISO/IEC 27001 certified. Krones policies and guidelines are based on international standards and best practice methodologies to ensure an adequate level of information security. The company complies with personal data protection regulations, in particular as defined in GDPR to the extent that this legislation is applicable.

To fulfill the requirements according to article 32 GDPR the following technical and organizational measures have been implemented.

## I. Principles Pseudonymization, Encryption, Information Security and Data Protection by Design

According to the principles of pseudonymization and anonymization, and to the extent that individual-related data is not necessary for the purpose of a processing activity, data is processed and used in non-individual-related form. The usage of state of the art encryption technologies is based on the internal information use policy and guidelines for the usage of cryptographic algorithms. The involvement of information security and data protection requirements in the design and change of services at an early stage ("security & privacy by design") ensures measures and a level of security appropriate to the risk.

## II. Securing of Confidentiality, Integrity and Availability of data

Krones AG has taken the following measures to ensure the protection objectives of confidentiality, integrity and availability.

**1) Measures regarding confidentiality**

**Physical access control**

Physical access to data processing systems with which personal data are processed and used is denied for unauthorized persons.

Measures:

- Access to business premises and data centers only for authorized persons
- Business premises are guarded by plant security
- Electronic access control via identity card with transponder chip
- Management of all access rights with an access control system
- Access to data centers only with two-factor authentication
- Intrusion detection system for the data centers

- Access authorization process for externals (documentation of permission and handover of identity card)

**IT system access control**

Prevention of access to data processing systems for use by unauthorized persons.

Measures:

- Access to servers and clients with authentication via individual user ID and password (enforced Password Security Policy)
- Password Security Guideline according to Best Practice with complexity requirements and regular password changes
- Protection of the internal network against unauthorized access with firewall and antivirus software
- Access to clients via remote service only for authorized persons and with approval of the user
- Remote access to the internal network only via VPN/Citrix by using two-factor authentication
- Usage of a Mobile Device Management System

**Data access control**

Persons authorized to use an automated processing system have access only to the personal data covered by their access authorization.

Measures:

- Rights- and role-based access control system
- Assignment of permissions according to need to know principle
- Centralized authorization management and identity and access management with appropriate processes
- Separate personal accounts for administrative purposes
- Access logging
- Backup and restore concept
- Regular internal and external audits to review the measures for access control

**Separability**

Personal data collected for different purposes can be processed separately.

Measures:

- Logically separated storage of data from different customers in our digital services
- Regulation of access rights based on group guidelines and directory structures

**2) Measures regarding Integrity**

**Transmission Control**

Personal data cannot be read, copied, modified or removed during electronic transmission or during transport of data storage media.

Measures:

- Disposal of storage media and information by a certificated specialist
- Encrypted media devices by using state-of-the-art procedures
- Classification Levels for information and appropriate handling according to guidelines
- Encrypted VPN connections
- Transmission of data via encrypted connections (e.g. TLS)
- Optional solution for e-mail-encryption

**Input Control**

It is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input.

Measures:

- Logging of sensitive actions and events in critical systems
- Authentication via individual user ID

- Differentiated assignment of authorizations

**3) Measures regarding Availability, Resilience and Recovery**

**Securing of Availability**

Personal data are protected against loss and destruction.

Measures:

- Physical security of the data centers (e.g. UPS, fire protection, intrusion detection system, refrigeration plant)
- Redundant data centers
- Redundant power supply and network connection of the data centers
- Hardware and software protection (e.g. virus scanner, firewall, UPS redundant, refrigeration plant)
- Secure deletion and disposal of data carriers and it devices based on internal guideline for the secure deletion and erasure (based on DIN-66399)

**Recovery of Availability**

Installed systems may, in the case of interruption, be restored.

Measures:

- IT Service Continuity Management processes and regular emergency drills
- Emergency and recovery plans for central IT-services
- Backup and restore concept with daily data backup

## III. Processes for regularly testing, assessing and evaluating of technical and organizational measures

**Information Security- and Data Protection Management System**

The implemented technical and organizational security measures are tested, assed and evaluated on a regular basis within the ISMS and DPMS to guarantee a continuous improvement.

Measures:

- ISMS based on ISO 27001 and IT Service Management based on ISO 20000
- Information Security Policy as top-level document with detailed sub-policies for all relevant areas
- Internal and external audits to test, assess and evaluate the implemented technical and organizational measures on a regular basis
- Technical review and maintenance for central it systems on a regular basis
- Vulnerability and penetration tests for it systems by our internal security team and with external partners
- Information Security Incident Response Process and Team (ISIRT) to handle and coordinate security incidents
- Product Security Incident Response Team (PSIRT) to handle and coordinate product related security events and incidents and to provide security advisories to customers
- Continous improvement process for our management system

**Processing Control**

Personal data processed on behalf of the controller can only be processed in compliance with the controller´s instructions.

Measures:

- Supplier Management process and process for the evaluation and selection of suppliers, especially guidelines for the usage of cloud services and checklists for provider of cloud services
- Contacts and order confirmations have to be provided in writing and have to include the duties, tasks and guidelines of the customer and the supplier
- Employees employed in processing are informed about the customers specification and the specific working instructions
- Employees employed in processing are obligated to confidentiality and regular instructed on data protection and information security

- Data protection agreements with subprocessors involved in the processing of personal data according to art. 28 GDPR and/or agreement based on appropriate safeguards and guarantees for processing activities by subprocessors located in a third country (see art. 28 sec. 4)

KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

# Part B - Service specific technical and organizational security measures (STOMs)

## STOMs for LCS Support

KRONES AG relies on a multi-level concept for the provision of the Argos (Augmented Reality Support) and GRS (Global Remote Service) IT services. The majority of the GRS (Global Remote Service) IT service is provided on servers operated at the KRONES AG data center. Individual parts of the IT service Argos (Augmented Reality Support) and GRS (Global Remote Service) will be procured as "Managed Services" from third parties. Remote service is provided by KRONES AG employees specially trained for remote service. In order to achieve a high level of data security KRONES AG carefully selects its suppliers, concludes data processing agreements with those suppliers and monitors compliance with them as part of its ISMS activities.

## STOMs for Digital Services

Share2Act Digital Services are developed and operated by Syskron GmbH on behalf of Krones AG. Share2Act Digital Services are built on Platform and Services provided by Amazon Web Services. For the protection of personal data within Share2Act Digital Services Syskron has implemented a comprehensive set of technical and organizational measures.

### I. Principles Pseudonymization, Encryption, Information Security and Data Protection by Design

According to the principles of pseudonymization and anonymization, and to the extent that individual-related data is not necessary for the purpose of a processing activity, data is processed and used in non-individual-related form. The usage of state of the art and best practice encryption technologies is based on the internal information use policy and guidelines for the usage cryptographic algorithms. The involvement of information security and data protection requirements in the design and change of services at an early stage (“security & privacy by design”) ensures measures and a level of security appropriate to the risk.

### II. Securing of Confidentiality, Integrity and Availability of data

The following measures have been taken to ensure the protection objectives of confidentiality, integrity and availability.

**Data access control**

Persons authorized to use an automated processing system have access only to the personal data covered by their access authorization.

Measures:

- Assignment of permissions according to need to know principle
- Separate personal accounts for administrative purposes
- Backup and restore concept

**Separability**

Personal data collected for different purposes can be processed separately.

Measures:

- Logically separated storage of data from different CUSTOMERS.
- Concept and structure for access control and tenants.

**Input Control**

It is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input.

Measures:

- Logging and needs-based provision of corresponding actions carried out on systems (e.g. log files)
- Authentication via individual user ID
- Differentiated assignment of authorizations

**Securing of Availability**

Personal data are protected against loss and destruction.

Measures:

- Redundant data center of our hosting partners
- Redundant data storage of our hosting partners
- Deletion of data according to legal requirements and customer demands

**Resilience of Systems**

We take preventive measures, which are already contributing to stability of systems before implementation of data processing by the processors.

Measures:

- Usage of load balancing of network traffic on the server
- Execute recurring penetration tests against the data processing systems
- Automated adjustment of computing power, storage and random-access memory

**Recoverability of availability**

We assure the availability through recoverability by implemented disaster recovery plans.

Measures:

- Archiving and separately storing of data sets on a regularly basis in combination with server mirroring of our hosting partner
- Backup concept with daily data backup

## III. Processes for regularly testing, assessing and evaluating of technical and organizational measures

We implement measures to examine and keep the existing technical and organizational measures up to date.