Kordiam GDPR Documentation -
Technical and Organisational Measures
Annex to the Kordiam Data Processing Agreement

Introductory Comments

The below-mentioned measures relate to tasks performed by the Kordiam GmbH. These are user support and product development tasks.

Operations, maintenance, development and testing of the Kordiam application are performed by partner companies with whom the necessary agreements have been entered.

More information on these partners can be found in the Data Processing Agreement and on https://kordiam.io/gdpr.

The structure of the content below is derived from Art. 32 (1) GDPR.

Anonymization and Encryption

- Encrypted data transfer between client and server (SSL, RSA 2048 bits)
- Encryption at rest of data
- Anonymization of personal data for development and related testing purposes

Confidentiality

- Rigorous office access concept including multiple locked doors with keys distributed only to regular employees and cleaning staff.
- Access to the office for visitors only accompanied by an employee
- Locking concept for windows
- Documented system access concept including user access removals with regular reviews
- Usage of anti-virus software including automated updates
- Automatically activated and password-protected computer locking
- Secure and regularly updated passwords with very limited set of employees receiving them
- Two different sets of login credentials needed to access customer data
- No access to personal data in a non-authenticated way
- Prevention of brute force password entry attempts to Kordiam
- Restriction to account access to company network for Kordiam customers possible
- Default and enhanced password requirements available
- Logging of accesses (including failed ones) to the application
- Detailed process in place with customers to ensure data is only edited based on individual written requests by eligible persons on the customer side
- Separated handling of customer data
- No usage of mobile data storage mediums

Integrity

- Detailed tracking of entries, edits and deletions
- Regular data backups to ensure availability of an uncorrupted database version
- Logical client separation in the application

- Separation of production, text and development systems
- Regular updates and patches of external software components

Availability and Resilience

- Documented incident response processes
- High-availability domain hosting
- Redundant databases
- Multiple data backups per day
- Backup of short-term planning data in xls format to customer ftp server
- Deletion procedures
    - The controller is responsible for deleting individual user profiles and their related data during the duration of the Kordiam contract.
    - The data processor deletes the controller’s user profiles within 90 days of the end of the contract.
    - Backups which may contain personal data that has been deleted from the production system are stored for a maximum of six months.

Ability to Restore the Availability and Access to Personal Data

- Documented and regularly tested failover procedures
- Automation of processes to restore the application or parts of it

Processes for Regular Testing, Assessing and Evaluating the Effectiveness of Technical and Organizational Measures for Ensuring the Security of the Processing

- Regular review of data privacy measures
- Regular training of employees on data privacy measures
- Regular monitoring of partner companies regarding data privacy measures