

Misure tecniche e organizzative (TOM)

Aggiornamento: 1° ottobre 2026 · generato il 02 ottobre 2026

Questo documento è disponibile in inglese.

Taking into account the state of the art, the costs of implementation, and the nature, scope, circumstances, and purposes of Processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of data subjects, Logicc has implemented and will maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to maintain the security and confidentiality of Customer Data ("technical and organizational measures"). These measures include the following aspects:

1. Confidentiality

1.1 Physical access control

Logicc does not operate its own data centers or server rooms. The application is operated on cloud infrastructure in ISO/IEC 27001-certified data centers. Physical access control at the data centers is provided by the hosting providers in accordance with their contractually agreed technical and organizational measures. The following measures apply to Logicc's business premises:

- Digital access control system with individual access permissions for employees.
- Authentication using a personal access code or biometric factor.
- Logging of physical access events.
- Granting and revocation of physical access permissions according to operational requirements.
- Visitors and external service providers are admitted only by authorized employees and may not remain unattended in non-public areas.

1.2 System access control

Logicc will take appropriate measures to prevent unauthorized persons from using data processing systems.

- Technical measures:
- Use of individual user accounts and strong, unique authentication credentials.
- Use of multi-factor authentication or passkeys where technically supported, particularly for privileged or security-relevant access.
- Use of centrally approved password management to generate and securely store unique credentials.
- Change of credentials following known or suspected compromise or for other security-related reasons.
- Automatic locking of inactive sessions after a defined period.
- Central management of Logicc-provided endpoints to enforce and monitor security configurations, operating system updates, and device compliance.
- Full-disk encryption of Logicc-provided endpoints.
- Management of user permissions.

- Organizational measures:
- IT security policy governing the secure handling of passwords, credentials, and mobile devices.
- Use of Logicc-provided and centrally managed endpoints by employees when Processing Customer Data.
- Assignment of user accounts in accordance with the principle of least privilege.
- Regular security training for employees to raise awareness of phishing and other threats.

1.3 Data access control

Logicc will take appropriate measures to ensure that persons authorized to use the data processing systems can access only the Personal Data covered by their access authorization and that Customer Data cannot be read, copied, modified, or removed without authorization during Processing, use, or after storage. Logicc takes the following precautions:

- Technical measures:
- Implementation of a differentiated authorization concept that restricts access to Customer Data to the minimum necessary.
- Use of network and application filters, including a web application firewall for publicly accessible application endpoints.
- Comprehensive logging of all access to Customer Data in tamper-resistant audit logs in accordance with defined retention periods.
- Separate logging of security-relevant database access.
- Administrative access to hosting infrastructure only through encrypted and access-protected connections.
- Centralized, encrypted management of production secrets and cryptographic keys; access and provisioning are restricted to the persons and services that require them.
- Encryption of Customer Data at rest using strong, state-of-the-art encryption methods.
- Organizational measures:
- Policy for granting and revoking access rights based on the "need-to-know" principle.
- Regular and event-driven reviews of access permissions, particularly for privileged access.
- Specific authorization for access to particularly sensitive categories of data.
- Restriction of privileged access to a small group of persons for whom it is operationally necessary, in accordance with the principle of least privilege.
- Before being granted access, employees whose activities may give them knowledge of Customer Data are bound in text form to confidentiality and to protect third-party secrets pursuant to Section 203 of the German Criminal Code (StGB).

1.4 Separation control

Logicc will take appropriate measures to ensure that Customer Data collected for different purposes can be processed separately. Logicc takes the following precautions:

- Technical measures:
- Strict logical tenant separation within the central database through the use of Row-Level Security (RLS).
- Enforcement of tenant separation at the application level to prevent access to other tenants' data.
- Separate environments for development, testing, and production.

- A differentiated authorization concept governing access.
- Organizational measures:
- Policy on data classification and the separate Processing of data belonging to different tenants and purposes.
- Regular review of the technical and organizational measures for data separation.

2. Integrity

2.1 Transfer control

Logicc will take appropriate measures to reduce the risk that Customer Data may be read, copied, modified, or removed without authorization during electronic transmission or during its transport or storage on data carriers. Logicc takes the following precautions:

- Technical measures:
- Consistent encryption of all transmissions of Customer Data over external or public networks using at least TLS 1.3.
- Use of approved, access-protected transmission channels and cloud services for the exchange and provision of Customer Data.
- Organizational measures:
- Policy on the secure transfer and disclosure of Customer Data that prohibits the use of insecure channels.
- Employee awareness training on the risks of insecure data transmission.
- Clear rules on the use of cloud services and the transfer of data to third parties.
- Documented overview of regular retrieval and transmission procedures.

2.2 Input control

Logicc will take appropriate measures to ensure that it can subsequently be checked and determined whether and by whom Customer Data was entered into, modified in, or removed from data processing systems. Logicc takes the following precautions:

- Technical measures:
- Comprehensive logging of all entries, changes, and deletions of Customer Data in tamper-resistant audit logs in accordance with defined retention periods.
- Separate logging of security-relevant database access.
- Plausibility and validation checks during data entry.
- Traceability of changes through timestamps or versioning where technically provided for the relevant Processing operation.
- Organizational measures:
- Clear responsibilities for data entry and maintenance.
- Assignment of rights to enter, modify, and delete data based on an authorization concept.
- Regular and event-driven reviews of security-relevant logs.

3. Availability and resilience

Logicc will take appropriate measures to ensure that Customer Data is protected against accidental destruction or loss. Logicc takes the following precautions:

- Technical measures:
- Hosting of the application and Customer Data in ISO/IEC 27001-certified data centers.
- Daily backups of production Customer Data and of the systems and configurations required for secure operations.
- Storage of backups within the European Union and encryption using AES-256.
- Regular retention of backups for 14 days; deleted backups remain recoverable for 90 days through a soft-delete function.
- During the soft-delete period, deleted backups are retained solely for disaster recovery purposes, are not used in production, and are automatically and permanently deleted after the period expires.
- Monitoring of backup processes and regular review and documentation of backup results.
- Regular and event-driven testing of backup recoverability, at least once per quarter.
- Technical measures to detect and defend against malware and other security threats.
- Physical protection and redundancy measures implemented by the data center operators, particularly for power supply, air conditioning, fire protection, and storage systems.
- Organizational measures:
- Documented backup and recovery concept based on the criticality of the data and systems and defining responsibilities, escalation paths, and automation-supported recovery steps.
- Contingency plans for relevant failure scenarios that are regularly reviewed, updated, and tested.
- Designated internal persons responsible for emergencies, technical security incidents, and necessary recovery measures.
- Use of the contractually agreed standard availability and support services of the hosting providers.
- Information security policy containing requirements for availability, recovery, and emergency operations.

4. Procedures for regular review, assessment, and evaluation

Logicc implements procedures for regularly reviewing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of Processing.

4.1 Data protection management

- An external data protection officer has been appointed. The data protection officer is supported in implementing data protection measures within the company by the managing director and a designated employee, who act as internal data protection coordinators.
- Implementation of a data protection management system (DPMS) based on established standards (e.g., ISO 27701 and BSI IT-Grundschutz), adapted to the size and complexity of the company.
- Regular internal reviews of data protection measures and processes, at least once a year.
- Documentation and handling of data protection incidents in accordance with a defined internal process.
- Regular employee training on data protection, at least once a year.
- Processes implementing the information obligations pursuant to Articles 13 and 14 GDPR.
- Formalized procedure for requests from data subjects.
- Integration of data protection checkpoints into risk assessments where possible and appropriate.
- Data protection impact assessments (DPIAs) are conducted as necessary for new Processing activities likely to result in a high risk.

- Data protection considerations form part of the company's general risk management.

4.2 Incident response management

- Use of monitoring restricted to technical error and performance information, with measures to avoid capturing prompts, model responses, document content, authentication tokens, and full request bodies.
- Documented incident response process for detecting, reporting, analyzing, responding to, and following up on security incidents and Personal Data breaches, including assessment of statutory notification obligations.
- Designated internal incident response group and involvement of technical management in coordinating and handling security incidents and Personal Data breaches.
- Central documentation and tracking of security incidents and Personal Data breaches.
- Use of a web application firewall to protect publicly accessible application endpoints.
- Use of centralized spam, phishing, and malware protection mechanisms for business email communications.
- Regular employee training on handling security incidents and phishing attempts.
- Regular review and continuous improvement of the incident response procedure.

4.3 Secure software development and vulnerability management

- Protected development branches and controlled merge, approval, and release processes for changes to application code.
- Testing of changes in a test environment separated from production before deployment to production.
- Security, dependency, and vulnerability scans integrated into the development process and performed regularly.
- Identified vulnerabilities are prioritized according to severity and actual exposure and remediated promptly.