EXHIBIT 7

Technical and Organisational Measures (TOM)

Version 2026-07 · published at tchop.io/resources/security

Table of Contents

1. Pseudonymisation 2
2. Encryption 2
3. Guaranteeing Confidentiality 2
   3.1 Physical Access Control 2
   3.2 System Access Control 3
   3.3 Data Access Control 3
4. Guaranteeing Integrity 4
5. Separation Control 4
6. Guaranteeing Availability 4
   6.1 System Availability 4
   6.2 Data Availability 4
7. Deletion of Data 5
8. Guaranteeing System Resilience 5
9. Procedures for Regular Review, Assessment and Evaluation 5

tchop confirms that it has implemented measures to comply with the requirements pertaining to the security of processing pursuant to Art. 32 GDPR. These measures form part of tchop's information security management system (ISMS), which is certified according to ISO/IEC 27001 (certified by TÜV Süd, since 2021), and are continuously developed further.

The tchop platform is operated in certified data centres within the European Union, currently on the cloud infrastructure of Amazon Web Services in the Frankfurt am Main region (eu-central-1). An alternative hosting option with a German infrastructure provider can be agreed contractually. tchop does not operate any local servers of its own; no customer data is stored on tchop's business premises. The subprocessors engaged are listed in Exhibit 6 of the Enterprise Platform Agreement; the current list is also published at tchop.io/resources/security.

1. Pseudonymisation

- Each user is automatically assigned a unique, random user ID; in logs, interfaces and internal system components, users are represented exclusively by this ID.
- The mapping of name and e-mail address to the user ID is stored encrypted in the database; access is restricted to a small number of authorised employees (see Access Control).
- Usage analytics are performed exclusively on an anonymised basis; no personal usage profiles are created (see Separation Control).

2. Encryption

- Encryption in transit: all communication over public networks takes place exclusively via HTTPS with TLS 1.2 or higher and Perfect Forward Secrecy; insecure protocol versions are disabled.
- Encryption at rest: all data stored on AWS is encrypted server-side with AES-256; key management is provided by the cloud provider with regular key rotation; access to key management is restricted to the management and technical lead.
- Passwords are stored exclusively as one-way hashes (bcrypt) and never exist in plain text; a reset is only possible via the “forgotten password” function with an e-mail link.
- Minimum requirements apply when passwords are created (minimum length, strength indicator) to guide users towards passwords that are as secure as possible.
- Two-factor authentication (MFA) is available and can be activated or enforced at organisation level; in addition, app lock, session expiry and password policies are available as security settings.
- The real-time chat is end-to-end encrypted (AES-256, TLS 1.2+); chat messages and history are stored exclusively in encrypted form on European servers.
- All backups are encrypted (see Data Availability).

3. Guaranteeing Confidentiality

3.1 Physical Access Control

tchop business premises (Berlin):

- No servers are located, and no customer data is stored, on the business premises; all data resides in the data centres described below.
- Access to the premises is secured by an electronic locking system; access authorisations are managed centrally and withdrawn without delay when employees leave.
- Visitors are only granted access when accompanied by employees.
- All employees are obliged, through data protection training, to protect personal and confidential data against unauthorised access.

Data centres (AWS):

- Housed in nondescript buildings with physical security measures against unauthorised access (perimeter and building protection).
- Electronic access controls with alarm systems; video surveillance of sensitive areas; trained security staff around the clock (24/7).
- Visitors must identify themselves, are registered and are accompanied at all times.
- Access authorisations are approved by authorised persons and withdrawn within 24 hours of an employee or supplier record being deactivated.

3.2 System Access Control

- The principle of least privilege applies throughout: each user receives only the rights required for their work.
- User and administrator access to the cloud infrastructure is based on a role-based permission model with unique user identifiers.
- Provisioning and de-provisioning are linked to HR processes; access rights are withdrawn without delay when an employee record is deactivated.
- Binding conventions apply to employee passwords (minimum length, complexity); passwords are not stored in plain text anywhere.
- No personal customer data is stored on workstation computers; all laptops are fully encrypted; password-protected screen locks are mandatory.
- Access to production and test systems takes place exclusively via VPN with key-based authentication; communication within the cloud network is SSH-encrypted via a bastion host, which restricts access and logs activities for security audits.
- Firewalls at network and cloud level restrict access to the data processing environment; firewall configurations can only be changed by an authorised group of persons and are logged.

3.3 Data Access Control

- IAM users with restricted rights are used for day-to-day work; unrestricted root access to the cloud account rests exclusively with the management and is not used for day-to-day development.
- Access to relevant system components and services (including monitoring) is protected by IP whitelisting.
- Direct external access to user data in the database is not possible; access takes place exclusively via the cloud provider’s access and control system.
- Granted access rights to all relevant systems are reviewed at least quarterly by the technical lead.
- The creation, modification and deletion of user IDs and login credentials is logged with timestamps.
- Copying of data is only permitted within the scope of backups and specifically regulated cases of data transfer.
- A documented incident response plan governs responsibilities and procedures in the event of security incidents; a SIEM system collects and correlates system logs and alerts the team.

4. Guaranteeing Integrity

- All data interfaces and websites communicate exclusively via HTTPS.
- Content retrieval by the native apps and third-party systems takes place exclusively with authentication tokens (bearer tokens); tokens can be managed and revoked in the backend.
- Administrators and editors repeatedly identify themselves for backend access using their credentials; sessions expire configurably.
- Decommissioned storage media are securely taken out of service by the cloud provider according to documented procedures, so that recovery of data is excluded.
- The cloud environment has a limited number of controlled access points; administrative changes are logged.

5. Separation Control

- The technical architecture is modular; application and database layers are separated.
- Personal data (name, e-mail address) is stored in a separate, encrypted database, segregated from content data.
- The platform is multi-tenant; the data of different clients is processed with logical separation.
- Test, staging and production environments are logically separated from one another; the corporate network is separated from the production systems.
- Principle of data minimisation: no personal data is collected regarding the use of content (e.g. what individual users read); analyses are performed on an anonymised basis.
- A differentiated permission and role concept governs access at organisation and channel level (see Exhibit 2, User Management).

6. Guaranteeing Availability

6.1 System Availability

- The platform is continuously monitored through automated monitoring and alerting at the level of individual services and endpoints (24/7); failures of central components trigger automatic notifications to the engineering team.
- All production services are deployed at least redundantly (dual mode); if individual components fail, automatic failover takes place.
- DDoS attacks are mitigated by multiple tools, including AWS Shield with always-on detection and automatic inline mitigations.
- Development follows a test-driven continuous integration approach: automated tests and peer reviews of all code changes before production deployment; rollbacks are possible at short notice.
- Access to the monitoring systems is protected by a permission concept and IP whitelisting.

6.2 Data Availability

- Automated, encrypted backups of the entire database are performed daily; the retention period is configurable between 1 and 35 days.

- Backups enable point-in-time recovery; backups are kept separately from the production instance.
- Responsibilities for data backups are contractually regulated between tchop and the cloud provider (see Exhibit 6).

7. Deletion of Data

- The Company's administrators can independently retrieve, correct and delete user data at any time via the user management; after deletion, further processing is no longer possible.
- At the Company's request, tchop deletes defined data (individual users, channels or entire accounts) following an agreed procedure: definition of the data to be deleted, agreement on timing, review of statutory retention obligations.
- Upon termination of the agreement, all personal data is deleted or returned in accordance with the provisions of the Data Processing Agreement; copies in backup systems are deleted within the regular backup cycles.
- Personal data is never printed at tchop and at no time exists in paper form.
- Decommissioned hardware is professionally erased or destroyed in a data-protection-compliant manner before disposal.

8. Guaranteeing System Resilience

- The cloud architecture scales with increased request volumes; capacities are continuously monitored and expanded when defined limits are reached (see Exhibit 3, Capacity Management).
- Access to the data interface is protected by tokens, excluding uncontrolled access by third parties.
- Targeted denial-of-service attacks are mitigated, among other measures, by AWS Shield.

9. Procedures for Regular Review, Assessment and Evaluation

- tchop's ISMS is certified according to ISO/IEC 27001 and is reviewed in regular external audits (TÜV Süd).
- Vulnerability management and penetration testing: security vulnerabilities are systematically identified, assessed and remediated; a developer team under the supervision of the technical lead is responsible for this process.
- All code changes undergo automated tests and peer reviews (four-eyes principle).
- All employees are regularly trained in data protection and information security and are bound to confidentiality.
- At the end of each year, an additional external analysis of architecture and security measures is performed.
- The effectiveness of the measures described in this document is reviewed on an ongoing basis; the document is updated in the event of material changes.

Documentation as of: July 2026

_____

Signature, Management tchop GmbH