Technische und organisatorische Maßnahmen (TOM)

Version 2026-07 · veröffentlicht unter tchop.io/resources/security

Inhaltsverzeichnis

tchop bestätigt, Maßnahmen zur Einhaltung der Anforderungen an die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO ergriffen zu haben. Diese Maßnahmen sind Bestandteil des nach ISO/IEC 27001 zertifizierten Informationssicherheits-Managementsystems (ISMS) von tchop (zertifiziert durch TÜV Süd, seit 2021) und werden fortlaufend weiterentwickelt.

Die tchop Plattform wird in zertifizierten Rechenzentren innerhalb der Europäischen Union betrieben, derzeit auf der Cloud-Infrastruktur von Amazon Web Services in der Region Frankfurt am Main (eu-central-1). Eine alternative Hosting-Option bei einem deutschen Infrastrukturanbieter kann vertraglich vereinbart werden. tchop betreibt keine eigenen lokalen Server; in den Geschäftsräumen von tchop werden keine Kundendaten gespeichert. Die eingesetzten Subunternehmer sind in Anlage 6 des Enterprise Platform Agreement aufgeführt; die aktuelle Liste ist zudem unter tchop.io/resources/security veröffentlicht.

1. Pseudonymisierung

- Jede*r Nutzer*in erhält systemseitig eine eindeutige, zufällige Nutzer-ID; in Logs, Schnittstellen und internen Systemteilen werden Nutzer*innen ausschließlich über diese ID repräsentiert.
- Die Zuordnung von Name und E-Mail-Adresse zur Nutzer-ID ist verschlüsselt in der Datenbank gespeichert; Zugriff darauf haben nur wenige berechtigte Mitarbeiter*innen (siehe Zugriffskontrolle).
- Nutzungsanalysen erfolgen ausschließlich anonymisiert; es werden keine personenbezogenen Nutzungsprofile erstellt (siehe Trennungskontrolle).

2. Verschlüsselung

- Transportverschlüsselung: sämtliche Kommunikation über öffentliche Netze erfolgt ausschließlich über HTTPS mit TLS 1.2 oder höher und Perfect Forward Secrecy; unsichere Protokollversionen sind deaktiviert.
- Verschlüsselung im Ruhezustand: alle bei AWS gespeicherten Daten sind serverseitig mit AES-256 verschlüsselt; die Schlüsselverwaltung erfolgt über den Cloud-Anbieter mit regelmäßigem Schlüsselwechsel; Zugriff auf die Schlüsselverwaltung hat nur die Geschäftsführung bzw. technische Leitung.
- Passwörter werden ausschließlich als Einweg-Hash (bcrypt) gespeichert und liegen zu keinem Zeitpunkt im Klartext vor; ein Zurücksetzen ist nur über die „Passwort vergessen"-Funktion per E-Mail-Link möglich.
- Bei der Passwortvergabe gelten Mindestanforderungen (Mindestlänge, Stärke-Indikator), um Nutzer*innen zu möglichst sicheren Passwörtern anzuleiten.
- Zwei-Faktor-Authentifizierung (MFA) steht zur Verfügung und kann auf Organisationsebene aktiviert bzw. erzwungen werden; ergänzend stehen App Lock, Session-Ablauf und Passwort-Policies als Sicherheitseinstellungen bereit.
- Der Real Time Chat ist Ende-zu-Ende-verschlüsselt (AES-256, TLS 1.2+); Chat-Nachrichten und -Historie werden ausschließlich verschlüsselt auf europäischen Servern gespeichert.
- Alle Backups sind verschlüsselt (siehe Datenverfügbarkeit).

3. Gewährleistung der Vertraulichkeit

3.1 Zutrittskontrolle

Geschäftsräume von tchop (Berlin):

- In den Geschäftsräumen befinden sich keine Server und keine Speicherung von Kundendaten; sämtliche Daten liegen in den unten beschriebenen Rechenzentren.
- Der Zugang zu den Geschäftsräumen ist durch ein elektronisches Schließsystem gesichert; Zutrittsberechtigungen werden zentral verwaltet und bei Ausscheiden von Mitarbeiter*innen unverzüglich entzogen.
- Besucher*innen erhalten nur in Begleitung von Mitarbeiter*innen Zutritt.

- Alle Mitarbeiter*innen sind im Rahmen von Datenschutzunterweisungen verpflichtet, personenbezogene und vertrauliche Daten vor unberechtigtem Zugriff zu schützen.

Rechenzentren (AWS):

- Unterbringung in unauffälligen Gebäuden mit physischen Sicherheitsmaßnahmen gegen unberechtigten Zutritt (Perimeterschutz, Gebäudeschutz).
- Elektronische Zutrittskontrollen mit Alarmierung; Videoüberwachung sensibler Bereiche; ausgebildetes Sicherheitspersonal rund um die Uhr (24/7).
- Besucher*innen müssen sich ausweisen, werden registriert und stets begleitet.
- Zutrittsberechtigungen werden von autorisierten Personen genehmigt und nach Deaktivierung eines Mitarbeiter- oder Lieferantendatensatzes innerhalb von 24 Stunden entzogen.

3.2 Zugangskontrolle

- Es gilt durchgängig das Prinzip der minimalen Berechtigung: jede*r Nutzer*in erhält nur die für die Tätigkeit erforderlichen Rechte.
- Benutzer- und Administratorzugriff auf die Cloud-Infrastruktur beruht auf einem rollenbasierten Berechtigungsmodell mit eindeutigen Nutzerkennungen.
- Provisionierung und Deprovisionierung sind an das Personalwesen gekoppelt; Zugriffsrechte werden bei Deaktivierung eines Mitarbeiterdatensatzes unverzüglich entzogen.
- Für Mitarbeiter-Passwörter gelten verbindliche Konventionen (Mindestlänge, Komplexität); Passwörter werden an keiner Stelle im Klartext gespeichert.
- Auf Arbeitsplatzrechnern werden keine personenbezogenen Kundendaten gespeichert; alle Notebooks sind vollständig verschlüsselt; passwortgeschützte Bildschirmsperren sind verpflichtend aktiviert.
- Der Zugriff auf Produktions- und Testsysteme erfolgt ausschließlich über VPN mit schlüsselbasierter Authentifizierung; die Kommunikation im Cloud-Netzwerk erfolgt SSH-verschlüsselt über einen Bastion-Host, der Zugriffe beschränkt und für Sicherheitsaudits protokolliert.
- Firewalls auf Netzwerk- und Cloud-Ebene beschränken den Zugriff auf die Datenverarbeitungsumgebung; Firewall-Konfigurationen können nur durch einen autorisierten Personenkreis geändert werden und werden protokolliert.

3.3 Zugriffskontrolle

- Für die tägliche Arbeit werden IAM-Nutzer mit eingeschränkten Rechten verwendet; uneingeschränkter Root-Zugriff auf das Cloud-Konto liegt ausschließlich bei der Geschäftsführung und wird nicht für die tägliche Entwicklung genutzt.
- Zugriff auf relevante Systembestandteile und Dienste (u. a. Monitoring) ist durch IP-Whitelisting geschützt.
- Ein direkter Zugriff auf Nutzerdaten in der Datenbank von außen ist nicht möglich; der Zugriff erfolgt ausschließlich über das Zugangs- und Kontrollsystem des Cloud-Anbieters.
- Erteilte Zugriffsrechte werden mindestens vierteljährlich durch die technische Leitung überprüft.

- Das Erstellen, Ändern und Löschen von Nutzerkennungen und Anmeldeinformationen wird mit Zeitstempel protokolliert.
- Das Kopieren von Daten ist nur im Rahmen der Datensicherung und besonders geregelter Fälle der Datenweitergabe zulässig.
- Ein dokumentierter Vorfallreaktionsplan (Incident Response) regelt Zuständigkeiten und Abläufe bei Sicherheitsvorfällen; ein SIEM-System sammelt und korreliert Systemlogs und alarmiert das Team.

4. Gewährleistung der Integrität

- Sämtliche Datenschnittstellen und Websites kommunizieren ausschließlich über HTTPS.
- Die Abfrage von Inhalten durch die nativen Apps und Drittsysteme erfolgt ausschließlich mit Authentifizierungs-Token (Bearer Token); Token können im Backend verwaltet und entzogen werden.
- Administratoren und Redakteur*innen identifizieren sich für den Backend-Zugang wiederholt über ihre Zugangsdaten; Sitzungen laufen konfigurierbar ab.
- Ausgemusterte Speichermedien werden vom Cloud-Anbieter nach dokumentierten Verfahren sicher außer Betrieb genommen, so dass eine Wiederherstellung von Daten ausgeschlossen ist.
- Die Cloud-Umgebung verfügt über eine beschränkte Anzahl kontrollierter Zugangspunkte; administrative Änderungen werden protokolliert.

5. Trennungskontrolle

- Die technische Architektur ist modular aufgebaut; Anwendungs- und Datenbankebene sind getrennt.
- Personenbezogene Daten (Name, E-Mail-Adresse) werden in einer separaten, verschlüsselten Datenbank getrennt von Inhaltsdaten gespeichert.
- Die Plattform ist mandantenfähig; die Daten verschiedener Auftraggeber werden logisch getrennt verarbeitet.
- Test-, Staging- und Produktivumgebungen sind logisch voneinander getrennt; das Unternehmensnetzwerk ist von den Produktionssystemen getrennt.
- Grundsatz der Datensparsamkeit: zur inhaltlichen Nutzung des Angebots (z. B. was einzelne Nutzer*innen lesen) werden bewusst keine personenbezogenen Daten erhoben; Auswertungen erfolgen anonymisiert.
- Ein differenziertes Berechtigungs- und Rollenkonzept regelt die Zugriffe auf Organisations- und Kanalebene (siehe Anlage 2, Nutzerverwaltung).

6. Gewährleistung der Verfügbarkeit

6.1 Systemverfügbarkeit

- Die Plattform wird kontinuierlich durch automatisiertes Monitoring und Alerting auf Ebene einzelner Dienste und Endpunkte überwacht (24/7); Ausfälle zentraler Komponenten führen zu automatischen Benachrichtigungen an das Technik-Team.
- Alle produktiven Dienste sind mindestens redundant (dual) ausgelegt; bei Ausfall einzelner Komponenten erfolgt ein automatischer Failover.
- DDoS-Angriffe werden durch mehrere Werkzeuge mitigiert, darunter AWS Shield mit permanenter Erkennung und automatischen Inline-Mitigationen.
- Die Entwicklung folgt einem testgetriebenen Continuous-Integration-Ansatz: automatisierte Tests und Peer-Reviews aller Code-Änderungen vor Produktivstellung; Rollbacks sind kurzfristig möglich.
- Zugang zu den Monitoring-Systemen ist durch Berechtigungskonzept und IP-Whitelisting geschützt.

6.2 Datenverfügbarkeit

- Automatisierte, verschlüsselte Backups der gesamten Datenbank erfolgen täglich; der Aufbewahrungszeitraum ist zwischen 1 und 35 Tagen konfigurierbar.
- Backups ermöglichen eine Punkt-in-Zeit-Wiederherstellung; die Sicherungen werden getrennt von der Produktionsinstanz vorgehalten.
- Die Verantwortlichkeiten für die Datensicherung sind vertraglich zwischen tchop und dem Cloud-Anbieter geregelt (siehe Anlage 6).

7. Löschung von Daten

- Administrator*innen des Auftraggebers können Nutzerdaten jederzeit eigenständig über die Nutzerverwaltung abrufen, korrigieren und löschen; nach Löschung ist eine Weiterverarbeitung nicht mehr möglich.
- Auf Anforderung des Auftraggebers löscht tchop definierte Daten (einzelne Nutzer*innen, Kanäle oder gesamte Accounts) nach einem abgestimmten Verfahren: Definition der zu löschenden Daten, Abstimmung des Zeitpunkts, Prüfung gesetzlicher Aufbewahrungspflichten.
- Bei Beendigung des Vertrages werden alle personenbezogenen Daten gemäß den Regelungen des Auftragsverarbeitungsvertrages gelöscht bzw. zurückgegeben; Kopien in Backup-Systemen werden im Rahmen der regulären Backup-Zyklen gelöscht.
- Personenbezogene Daten werden bei tchop grundsätzlich nicht ausgedruckt und liegen zu keinem Zeitpunkt in Papierform vor.
- Ausgemusterte Hardware wird vor der Entsorgung fachgerecht und datenschutzkonform gelöscht bzw. vernichtet.

8. Gewährleistung der Belastbarkeit der Systeme

- Die Cloud-Architektur skaliert bei erhöhtem Anfragevolumen; Kapazitäten werden fortlaufend überwacht und bei Erreichen definierter Limits erweitert (siehe Anlage 3, Kapazitätsmanagement).
- Der Zugriff auf die Datenschnittstelle ist durch Token geschützt, so dass unkontrollierte Zugriffe Dritter ausgeschlossen sind.
- Gezielte Denial-of-Service-Angriffe werden u. a. durch AWS Shield mitigiert.

9. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Das ISMS von tchop ist nach ISO/IEC 27001 zertifiziert und wird im Rahmen regelmäßiger externer Audits (TÜV Süd) überprüft.
- Schwachstellenmanagement und Penetrationstests: Sicherheitslücken werden systematisch identifiziert, bewertet und behoben; ein Entwicklerteam unter Aufsicht der technischen Leitung verantwortet diesen Prozess.
- Alle Code-Änderungen durchlaufen automatisierte Tests und Peer-Reviews (Vier-Augen-Prinzip).
- Alle Mitarbeiter*innen werden regelmäßig zu Datenschutz und Informationssicherheit geschult und sind zur Vertraulichkeit verpflichtet.
- Zum Ende jedes Jahres erfolgt zusätzlich eine externe Analyse von Architektur und Sicherheitsmaßnahmen.
- Die Wirksamkeit der in diesem Dokument beschriebenen Maßnahmen wird fortlaufend überprüft; das Dokument wird bei wesentlichen Änderungen aktualisiert.

Stand der Dokumentation: Juli 2026

_____

Unterschrift Geschäftsführung tchop GmbH