

Technisch-organisatorische Maßnahmen

der Transaction-Network GmbH & Co. KG · nach Art. 32 DSGVO · Anlage TOM zur Vereinbarung zur Auftragsverarbeitung ·
Version 1.2, Stand: Oktober 2026

Maßgeblich ist die deutsche Fassung. Die englische Übersetzung folgt im Anschluss.

1. Allgemeines

Diese Technisch-organisatorischen Maßnahmen (TOM) beschreiben die Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 DSGVO für die SaaS-Plattform der Transaction-Network GmbH & Co. KG, die auf der Infrastruktur von Amazon Web Services (AWS) in Rechenzentren in Frankfurt am Main betrieben wird.

Der Betrieb erfolgt nach dem Shared-Responsibility-Modell:

- AWS verantwortet die physische Sicherheit der Rechenzentren sowie die Sicherheit der Cloud-Infrastruktur.
- Transaction-Network GmbH & Co. KG verantwortet die sichere Konfiguration, den Betrieb der Anwendungen, die Datenverarbeitung sowie organisatorische Maßnahmen.

2. Management und Organisation

- Externer Datenschutzbeauftragter (DSB): Rechtsanwalt Ulrich Emmert, e|s|b data GmbH, Stuttgart; aktive Unterstützung der Zusammenarbeit zwischen DSB und Informationssicherheitsbeauftragtem (ISB, Chief Technology & Security Officer) durch die Geschäftsleitung
- Sicherstellung der fachlichen Qualifikation des DSB sowie regelmäßige Fort- und Weiterbildungen
- Klare Definition und Dokumentation von Rollen und Verantwortlichkeiten (z. B. DSB, ISB, IT-Verantwortliche)
- Durchführung regelmäßiger Audits zur Überprüfung der Sicherheit der Verarbeitung gemäß Art. 32 DSGVO
- Integration der Informationssicherheit in alle unternehmensweiten Prozesse
- Laufende Analyse und Bewertung neuer digitaler Bedrohungen
- Einsatz eines angemessenen Informationssicherheitsmanagementsystems (z. B. ISO/IEC 27001 orientiert)
- Regelmäßige Überprüfung und Weiterentwicklung der Sicherheitsmaßnahmen nach dem PDCA-Zyklus
- Definition, Genehmigung und Kommunikation von Sicherheits- und Datenschutzrichtlinien
- Etablierte Eskalations- und Meldeprozesse bei Sicherheits- und Datenschutzvorfällen

3. Awareness und Schulungen

- Verpflichtung aller Mitarbeitenden auf Vertraulichkeit
- Regelmäßige Datenschutz- und Informationssicherheitsschulungen (mindestens jährlich)
- Schulungen für neue Mitarbeitende im Rahmen des Onboardings
- Sensibilisierung für Phishing, Social Engineering und sichere Passwortnutzung
- Spezifische Schulungen zur sicheren Arbeit im Homeoffice

4. Authentifizierung und Berechtigungen

- Einsatz starker Passwort-Richtlinien
- Passwortspeicherung ausschließlich mittels sicherer Hash-Verfahren (z. B. bcrypt mit Salt)
- Einsatz von Zwei-Faktor-Authentifizierung (2FA/MFA) für administrative und sicherheitskritische Zugriffe
- Zentrale Verwaltung von Benutzeridentitäten
- Automatische Sperrung von Benutzerkonten nach mehrfachen Fehlversuchen
- Trennung von Benutzer- und Administrationskonten

5. Rollen- und Berechtigungskonzept

- Umsetzung des Least-Privilege-Prinzips
- Rollenbasierte Zugriffskontrolle (RBAC) für interne Nutzer und Kunden
- Dokumentierte Prozesse zur Anlage, Änderung und Löschung von Benutzerkonten
- Regelmäßige Überprüfung der vergebenen Rollen und Berechtigungen

6. Netzwerk- und IT-Sicherheit (AWS)

- Betrieb der Plattform innerhalb logisch getrennter AWS Virtual Private Clouds (VPC)
- Netzwerksegmentierung durch Subnetze, Security Groups und Network ACLs
- Einsatz von virtuellen Firewalls und, sofern angemessen, Web Application Firewalls (WAF)
- Sperrung nicht benötigter Dienste und restriktive Konfiguration von Netzwerkzugriffen
- Ausschließliche Nutzung verschlüsselter Netzwerkprotokolle (TLS 1.2 oder höher)
- Regelmäßige Sicherheitsüberprüfungen, Schwachstellenscans und Penetrationstests

7. Server- und Plattformbetrieb

- Einsatz gehärteter Basis-Images und sicherer Standardkonfigurationen
- Regelmäßiges Patch- und Update-Management
- Einschränkung administrativer Zugriffe auf autorisierte und geschulte Personen
- Protokollierung administrativer Tätigkeiten
- Bevorzugte Nutzung von AWS Managed Services (z. B. RDS, S3)

8. Webanwendungen

- Absicherung von Webanwendungen gemäß anerkannten Standards (z. B. OWASP Top 10)
- Nutzung von HTTPS mit TLS 1.2 oder TLS 1.3
- Trennung von Webserver, Applikationslogik und Datenhaltung auf logischer Ebene
- Einschränkung und Absicherung von Administrationszugängen
- Regelmäßige Sicherheits- und Schwachstellentests

9. Entwicklung und Softwareauswahl

- Umsetzung von Privacy by Design und Security by Design
- Strikte Trennung von Entwicklungs-, Test- und Produktivumgebungen
- Regelmäßige Code-Reviews und Sicherheitsprüfungen
- Keine Speicherung von Zugangsdaten oder personenbezogenen Daten im Quellcode
- Regelmäßige Aktualisierung eingesetzter Frameworks und Bibliotheken

10. Protokollierung und Monitoring

- Zentrale Protokollierung sicherheitsrelevanter Ereignisse
- Synchronisierung der Systemzeiten
- Datenschutzkonforme Auswertung von Log-Daten
- Einsatz von Monitoring- und Alarmierungsmechanismen zur Vorfallerkennung

11. Archivierung und Datenmanagement

- Festlegung von Aufbewahrungsfristen und Rechtsgrundlagen
- Trennung von Archiv- und Produktivdaten
- Fristgerechte und nachvollziehbare Löschung archivierter Daten
- Sicherstellung der langfristigen Lesbarkeit archivierter Daten

12. Datensicherung und Business Continuity

- Regelmäßige Datensicherungen nach der 3-2-1-Regel
- Geografisch redundante Speicherung von Backups
- Dokumentierter Notfall- und Wiederanlaufplan inkl. Meldepflichten
- Schutzmaßnahmen gegen Ransomware (z. B. immutable Backups)
- Regelmäßige Tests der Wiederherstellbarkeit

13. Endgeräte und mobile Datenträger

- Verschlüsselung von Endgeräten und mobilen Datenträgern
- Regelmäßige Sicherheitsupdates und Patch-Management
- Einsatz von Virenschutz- und Endpoint-Protection-Lösungen
- Einschränkung und Regelung von BYOD und privater Gerätenutzung

14. Kryptografie und Datentransfer

- Verschlüsselung personenbezogener Daten bei Speicherung und Übertragung
- Einsatz starker kryptografischer Verfahren (z. B. AES-256, RSA-2048, SHA-256)
- Sichere Schlüsselverwaltung (z. B. AWS KMS)
- Transportverschlüsselung für alle externen und internen Datenübertragungen

15. Wartung durch externe Dienstleister

- Einsatz externer Dienstleister ausschließlich auf vertraglicher Grundlage
- Protokollierung und Kontrolle von Wartungs- und Supportzugriffen
- Verpflichtung externer Dienstleister zur Vertraulichkeit
- Regelungen zur sicheren Datenlöschung

16. Physische Sicherheit (AWS)

- Physische Sicherheitsmaßnahmen in AWS-Rechenzentren gemäß anerkannten Standards (z. B. ISO 27001)
- Zutrittskontrollen, Brandschutz, USV und Notfallkonzepte werden durch AWS umgesetzt
- Besuchermanagement und Gebäudeabsicherung liegen in der Verantwortung von AWS

17. Auftragsverarbeitung und Subdienstleister

- Abschluss eines Auftragsverarbeitungsvertrags (AVV) mit AWS
- Transparenz über eingesetzte Subdienstleister
- Regelungen zur Datenlöschung nach Vertragsende
- Einhaltung der DSGVO-Vorgaben bei internationalen Datentransfers

18. Überprüfung und Weiterentwicklung

- Regelmäßige Überprüfung der TOM auf Aktualität und Wirksamkeit
- Anpassung an neue rechtliche und technische Anforderungen
- Dokumentation aller Änderungen

Technical and Organisational Measures

of Transaction-Network GmbH & Co. KG · pursuant to Art. 32 GDPR · Annex TOMs to the Data Processing Agreement ·
Version 1.2, as of October 2026

English translation. Only the German version is legally binding.

1. General

These Technical and Organisational Measures (TOMs) describe the measures to ensure the security of processing pursuant to Art. 32 GDPR for the SaaS Platform of Transaction-Network GmbH & Co. KG, which is operated on the infrastructure of Amazon Web Services (AWS) in data centres in Frankfurt am Main.

Operation is based on the shared responsibility model:

- AWS is responsible for the physical security of the data centres and for the security of the cloud infrastructure.
- Transaction-Network GmbH & Co. KG is responsible for the secure configuration, the operation of the applications, the data processing and organisational measures.

2. Management and Organisation

- External data protection officer (DPO): attorney Ulrich Emmert, e|s|b data GmbH, Stuttgart; active support by the management for the cooperation between the DPO and the information security officer (Chief Technology & Security Officer)
- Ensuring the professional qualification of the DPO and regular training and further education
- Clear definition and documentation of roles and responsibilities (e.g. DPO, information security officer, persons responsible for IT)
- Regular audits to review the security of processing pursuant to Art. 32 GDPR
- Integration of information security into all company-wide processes
- Ongoing analysis and assessment of new digital threats
- Use of an appropriate information security management system (e.g. aligned with ISO/IEC 27001)
- Regular review and further development of the security measures in accordance with the PDCA cycle
- Definition, approval and communication of security and data protection policies
- Established escalation and reporting processes for security and data protection incidents

3. Awareness and Training

- Obligation of all employees to maintain confidentiality
- Regular data protection and information security training (at least annually)
- Training for new employees as part of onboarding
- Raising awareness of phishing, social engineering and secure use of passwords
- Specific training on working securely from home

4. Authentication and Permissions

- Use of strong password policies
- Storage of passwords exclusively by means of secure hashing methods (e.g. bcrypt with salt)
- Use of two-factor authentication (2FA/MFA) for administrative and security-critical access
- Central management of user identities
- Automatic locking of user accounts after multiple failed attempts
- Separation of user accounts and administrator accounts

5. Role and Permissions Concept

- Implementation of the principle of least privilege
- Role-based access control (RBAC) for internal users and Clients
- Documented processes for the creation, modification and deletion of user accounts
- Regular review of the roles and permissions assigned

6. Network and IT Security (AWS)

- Operation of the Platform within logically separated AWS Virtual Private Clouds (VPC)
- Network segmentation by means of subnets, Security Groups and Network ACLs
- Use of virtual firewalls and, where appropriate, Web Application Firewalls (WAF)
- Disabling of services that are not required and restrictive configuration of network access
- Exclusive use of encrypted network protocols (TLS 1.2 or higher)
- Regular security reviews, vulnerability scans and penetration tests

7. Server and Platform Operation

- Use of hardened base images and secure default configurations
- Regular patch and update management
- Restriction of administrative access to authorised and trained persons
- Logging of administrative activities
- Preferred use of AWS Managed Services (e.g. RDS, S3)

8. Web Applications

- Securing of web applications in accordance with recognised standards (e.g. OWASP Top 10)
- Use of HTTPS with TLS 1.2 or TLS 1.3
- Separation of web server, application logic and data storage at a logical level
- Restriction and securing of administrative access
- Regular security and vulnerability testing

9. Development and Software Selection

- Implementation of privacy by design and security by design
- Strict separation of development, test and production environments
- Regular code reviews and security checks
- No storage of access credentials or personal data in source code
- Regular updating of the frameworks and libraries used

10. Logging and Monitoring

- Central logging of security-relevant events
- Synchronisation of system times
- Evaluation of log data in compliance with data protection law
- Use of monitoring and alerting mechanisms for incident detection

11. Archiving and Data Management

- Definition of retention periods and legal bases
- Separation of archive data and production data
- Deletion of archived data within the applicable time limits and in a traceable manner
- Ensuring the long-term readability of archived data

12. Data Backup and Business Continuity

- Regular data backups in accordance with the 3-2-1 rule
- Geographically redundant storage of backups
- Documented emergency and recovery plan, including notification obligations
- Protective measures against ransomware (e.g. immutable backups)
- Regular testing of recoverability

13. End Devices and Mobile Storage Media

- Encryption of end devices and mobile storage media
- Regular security updates and patch management
- Use of anti-virus and endpoint protection solutions
- Restriction and regulation of BYOD and private device use

14. Cryptography and Data Transmission

- Encryption of personal data at rest and in transit
- Use of strong cryptographic methods (e.g. AES-256, RSA-2048, SHA-256)
- Secure key management (e.g. AWS KMS)
- Transport encryption for all external and internal data transmissions

15. Maintenance by External Service Providers

- Use of external service providers exclusively on a contractual basis
- Logging and control of maintenance and support access
- Obligation of external service providers to maintain confidentiality
- Rules on secure data deletion

16. Physical Security (AWS)

- Physical security measures in AWS data centres in accordance with recognised standards (e.g. ISO 27001)
- Physical access controls, fire protection, UPS and contingency plans are implemented by AWS
- Visitor management and building security are the responsibility of AWS

17. Processing on Behalf and Subcontractors

- Conclusion of a data processing agreement (DPA) with AWS
- Transparency regarding the subcontractors engaged
- Rules on data deletion after the end of the contract
- Compliance with GDPR requirements for international data transfers

18. Review and Further Development

- Regular review of the TOMs to ensure that they are up to date and effective
- Adaptation to new legal and technical requirements
- Documentation of all changes