

Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DSGVO · der Transaction-Network GmbH & Co. KG · gültig ab 1. November 2026

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

§ 1 Parteien, Gegenstand, Dauer

- (1) Auftragnehmer ist die Transaction-Network GmbH & Co. KG, Industriepark 312, 78244 Gottmadingen (TN). Auftraggeber ist der Kunde, mit dem TN einen Vertrag über die Nutzung der Plattform nach den AGB von TN oder über Leistungen nach den AGB Consulting schließt, der Enduser, der die Plattform nach den Enduser-Nutzungsbedingungen nutzt, sowie der Hersteller, der die Plattform nach den Freemium-Nutzungsbedingungen nutzt (Hauptvertrag). Der Kunde schließt diese Vereinbarung mit dem Hauptvertrag; Enduser und Hersteller nach den Freemium-Nutzungsbedingungen nehmen sie mit der Registrierung oder mit der Zustimmung zu einer neuen Fassung ihrer Nutzungsbedingungen an.
- (2) Diese Vereinbarung regelt die datenschutzrechtlichen Pflichten der Vertragsparteien, soweit TN personenbezogene Daten im Auftrag des Auftraggebers verarbeitet: bei der Bereitstellung der Plattform und bei Leistungen nach den AGB Consulting, bei denen TN personenbezogene Daten auf der Plattform oder in den Systemen des Auftraggebers verarbeitet. Gegenstand und Dauer ergeben sich im Übrigen aus dem Hauptvertrag; die AGB und die Nutzungsbedingungen sind unter www.transaction-network.com/agb abrufbar.
- (3) Die Vereinbarung läuft so lange wie der Hauptvertrag. Die Pflichten zur Rückgabe und Löschung (§ 4 Abs. 13) und zur Vertraulichkeit gelten darüber hinaus.

§ 2 Zweck, Art der Daten, betroffene Personen

- (1) Zweck der Verarbeitung ist die Bereitstellung und der Betrieb der Plattform gemäß ihren Funktionen sowie die Erbringung von Leistungen nach den AGB Consulting. Zu den Funktionen gehören insbesondere die Verwaltung von Maschinen und Dokumentation, Wartung, Serviceanfragen und die Kommunikation dazu, Bestellungen, Auswertungen, KI-Systeme nach § 11 der AGB und Support.
- (2) Art der Daten: Stamm- und Kontaktdaten von Nutzern (Vor- und Nachname, geschäftliche E-Mail-Adresse und Telefonnummer, Unternehmen, Funktion, Rolle); Zugangs- und Protokolldaten (Benutzerkennung, Anmeldezeitpunkte, IP-Adressen, Nutzungsprotokolle); Inhalte, die Nutzer einstellen (Serviceanfragen, Nachrichten, Wartungs- und Störungsberichte, Dokumente, Fragen an KI-Systeme und deren Antworten); Maschinendaten, soweit sie einer Person zugeordnet werden können (z. B. Bedienerkennungen). Geburtsdaten und soziodemografische Daten erhebt die Plattform nicht.
- (3) Betroffene Personen: Mitarbeiter des Auftraggebers und seiner verbundenen Unternehmen sowie Mitarbeiter von Herstellern, Servicepartnern, Lieferanten und Kunden des Auftraggebers, die er auf der Plattform einbindet.

§ 3 Verantwortlichkeit, Weisungen

- (1) Der Auftraggeber ist für die Einhaltung der gesetzlichen Regelungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenweitergabe an TN und der Datenverarbeitung, allein verantwortlich.
- (2) TN verarbeitet Daten nur im Rahmen des Auftrags und der Weisungen des Auftraggebers, sofern kein Fall des Art. 28 Abs. 3 lit. a DSGVO vorliegt. Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber in Schrift- oder Textform an die von TN bezeichnete Stelle geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich in Text- oder Schriftform zu bestätigen.
- (3) TN informiert den Auftraggeber unverzüglich, wenn eine Weisung nach Auffassung von TN gegen anwendbares Recht verstößt, und darf ihre Umsetzung aussetzen, bis der Auftraggeber sie bestätigt oder ändert.

§ 4 Pflichten des Auftragnehmers

- (1) Die Verarbeitung findet in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Eine Verarbeitung in einem Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (Angemessenheitsbeschluss oder geeignete

Garantien, etwa EU-Standardvertragsklauseln). Die Plattform und ihre KI-Systeme werden in Rechenzentren von Amazon Web Services in Frankfurt am Main betrieben.

- (2) TN gewährleistet die Sicherheit der Verarbeitung nach Art. 28 Abs. 3 lit. c und Art. 32 DSGVO durch die technischen und organisatorischen Maßnahmen der Anlage TOM. TN stellt die Anlage TOM auch als eigenes Dokument zum Download bereit. TN darf die Maßnahmen ändern, solange das vereinbarte Schutzniveau nicht unterschritten wird, und überprüft ihre Wirksamkeit regelmäßig (Art. 32 Abs. 1 lit. d DSGVO).
- (3) Zum Nachweis können genehmigte Verhaltensregeln nach Art. 40 DSGVO oder genehmigte Zertifizierungsverfahren nach Art. 42 DSGVO vorgelegt werden. Kann TN keine solchen Nachweise vorlegen, kann der Auftraggeber oder ein von ihm Beauftragter ein Audit durchführen.
- (4) TN gestaltet die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.
- (5) Inspektionen durch den Auftraggeber oder einen beauftragten Prüfer finden zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung mit angemessener Vorlaufzeit (mindestens 72 Stunden, werktäglich) statt. TN darf sie von einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden abhängig machen. Gegen einen Prüfer, der in einem direkten Wettbewerbsverhältnis zu TN steht, hat TN ein Einspruchsrecht.
- (6) Für Inspektionen einer Datenschutz- oder sonstigen Aufsichtsbehörde gilt Abs. 5 entsprechend; einer Verschwiegenheitserklärung bedarf es nicht, wenn die Behörde einer sanktionsbewehrten gesetzlichen Verschwiegenheit unterliegt.
- (7) TN unterrichtet den Auftraggeber unverzüglich über Verletzungen des Schutzes personenbezogener Daten des Auftraggebers und über Verstöße gegen datenschutzrechtliche Vorschriften durch TN, ihre Mitarbeiter oder sonstige Dritte, trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung nachteiliger Folgen und stimmt sich dazu mit dem Auftraggeber ab.
- (8) Werden die Daten des Auftraggebers durch Pfändung oder Beschlagnahme, ein Insolvenz- oder Vergleichsverfahren oder sonstige Maßnahmen Dritter gefährdet, informiert TN den Auftraggeber unverzüglich und alle Beteiligten darüber, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem liegen.
- (9) TN unterstützt den Auftraggeber im Rahmen ihrer Möglichkeiten und in notwendigem Umfang bei Anfragen und Ansprüchen betroffener Personen nach Kapitel III DSGVO und bei den Pflichten nach Art. 33 bis 36 DSGVO.
- (10) TN stellt sicher, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, auch über das Ende des Auftrags hinaus.
- (11) Ansprechpartner für Datenschutzfragen bei TN: Matthias Maier, Transaction-Network GmbH & Co. KG, Industriepark 312, 78244 Gottmadingen, Tel. +49 7731 16923-23, datenschutz@transaction-network.com. Datenschutzbeauftragter von TN ist Rechtsanwalt Ulrich Emmert, e|s|b data GmbH, Schockenriedstr. 8A, 70565 Stuttgart, info@esb-data.de, Tel. +49 711 46905830.
- (12) Personenbezogene Daten verwendet TN nicht zum Training von KI-Systemen; es gilt § 11 der AGB.
- (13) Nach Ende des Auftrags gibt TN Daten, Datenträger und sonstige Materialien auf Verlangen heraus oder löscht sie, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen; im Übrigen gilt die Regelung des Hauptvertrags zum Vertragsende (§ 7 der AGB, § 6 der Enduser-Nutzungsbedingungen, § 10 Abs. 2 der Freemium-Nutzungsbedingungen). Ein Zurückbehaltungsrecht besteht nicht. Eine Löschung oder Vernichtung, die über die übliche Löschung hinausgeht, erfolgt auf Einzelauftrag.
- (14) Wird der Auftraggeber von einer betroffenen Person nach Art. 82 DSGVO in Anspruch genommen, unterstützt TN ihn bei der Abwehr im Rahmen ihrer Möglichkeiten. Die Unterstützung vergütet der Auftraggeber nach den Sätzen der Preisliste; TN informiert ihn vorab und regelmäßig über den zu erwartenden Aufwand.

§ 5 Pflichten des Auftraggebers

- (1) Der Auftraggeber ist für die Rechtmäßigkeit der Datenweitergabe an TN und der Verarbeitung in seinem Verantwortungsbereich allein verantwortlich und genügt seiner Rechenschaftspflicht nach Art. 5 Abs. 2 und Art. 24 Abs. 1 DSGVO.

- (2) Er informiert TN unverzüglich, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.
- (3) Er benennt TN einen Ansprechpartner für Datenschutzfragen mit Kontaktdaten.

§ 6 Anfragen betroffener Personen

- (1) Macht eine Person gegenüber TN ein Betroffenenrecht nach Art. 12 ff. DSGVO geltend, leitet TN die Anfrage unverzüglich an den Auftraggeber weiter und unterstützt ihn in notwendigem und angemessenem Umfang.

§ 7 Unterauftragsverarbeiter

- (1) Der Auftraggeber erteilt TN die allgemeine Genehmigung, weitere Auftragsverarbeiter hinzuzuziehen. TN informiert den Auftraggeber vorher in Textform über die Hinzuziehung oder Ersetzung eines weiteren Auftragsverarbeiters; der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen.
- (2) Keine Unterauftragsverarbeiter sind Lieferanten, deren Leistungen sich nicht unmittelbar auf die Hauptleistung beziehen (z. B. Telekommunikation, Post- und Transportdienste, Entsorgung, Facility Management).
- (3) TN schließt mit Unterauftragsverarbeitern Vereinbarungen, die ihnen die datenschutzrechtlichen Pflichten dieser Vereinbarung übertragen und angemessene Datenschutz- und Sicherheitsmaßnahmen gewährleisten.

§ 8 Sonderkündigungsrecht

- (1) Der Auftraggeber kann den Hauptvertrag ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß von TN oder eines Unterauftragsverarbeiters gegen Datenschutzvorschriften oder gegen diese Vereinbarung vorliegt.
- (2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt sind oder Kontrollrechten des Auftraggebers nicht genügt wird. Bei sonstigen Verstößen setzt der Auftraggeber eine angemessene Frist zur Abhilfe; erfolgt sie nicht rechtzeitig, kann er nach Abs. 1 kündigen.

§ 9 Haftung

- (1) Im Verhältnis der Vertragsparteien gelten die Haftungsregelungen des Hauptvertrags (§ 13 der AGB, § 10 der AGB Consulting, § 8 der Enduser-Nutzungsbedingungen oder § 9 der Freemium-Nutzungsbedingungen). Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt.

§ 10 Schlussbestimmungen

- (1) In Fragen des Datenschutzes geht diese Vereinbarung dem Hauptvertrag vor; für die Haftung gilt § 9.
- (2) Sollten einzelne Regelungen unwirksam sein, bleibt die Wirksamkeit dieser Vereinbarung und des Hauptvertrags unberührt.
- (3) Es gilt deutsches Recht. Gerichtsstand ist Singen (Hohentwiel), soweit der Hauptvertrag dies vorsieht.
- (4) Diese Fassung gilt ab dem 1. November 2026 für Verträge, die ab diesem Tag geschlossen werden, und für Enduser und Hersteller, die einer ab diesem Tag gültigen Fassung ihrer Nutzungsbedingungen zustimmen. Im Übrigen gilt für bestehende Verträge die bisherige Vereinbarung fort.

Anlage TOM: Technisch-organisatorische Maßnahmen

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

Data Processing Agreement

pursuant to Art. 28 GDPR · of Transaction-Network GmbH & Co. KG · valid from 1 November 2026

English translation. Only the German version is legally binding.

Section 1 Parties, Subject Matter, Duration

- (1) The Processor is Transaction-Network GmbH & Co. KG, Industriepark 312, 78244 Gottmadingen (TN). The Controller is the Client with whom TN concludes a contract for the use of the Platform under TN's GTC or for services under the GTC Consulting, the End User who uses the Platform under the End User Terms of Use, and the Manufacturer who uses the Platform under the Freemium Terms of Use (Main Contract). The Client concludes this Agreement together with the Main Contract; End Users and Manufacturers under the Freemium Terms of Use accept it upon registration or upon agreeing to a new version of their terms of use.
- (2) This Agreement governs the data protection obligations of the parties to the extent that TN processes personal data on behalf of the Controller: in providing the Platform and in performing services under the GTC Consulting in the course of which TN processes personal data on the Platform or in the Controller's systems. In all other respects, the subject matter and duration follow from the Main Contract; the GTC and the terms of use are available at www.transaction-network.com/agb.
- (3) This Agreement shall remain in force for as long as the Main Contract. The obligations regarding return and deletion (Section 4 (13)) and confidentiality shall continue to apply thereafter.

Section 2 Purpose, Type of Data, Data Subjects

- (1) The purpose of the processing is the provision and operation of the Platform in accordance with its functions and the performance of services under the GTC Consulting. The functions include, in particular, the management of Machines and documentation, maintenance, service requests and related communication, orders, analyses, AI systems under Section 11 of the GTC, and support.
- (2) Type of data: master data and contact data of users (first name and surname, business email address and telephone number, company, job function, role); access and log data (user ID, login times, IP addresses, usage logs); content posted by users (service requests, messages, maintenance and fault reports, documents, questions put to AI systems and their answers); Machine data, to the extent that they can be attributed to a person (e.g. operator IDs). The Platform does not collect dates of birth or socio-demographic data.
- (3) Data subjects: employees of the Controller and of its affiliated companies, as well as employees of Manufacturers, service partners, suppliers and customers of the Controller whom the Controller involves on the Platform.

Section 3 Responsibility, Instructions

- (1) The Controller is solely responsible for compliance with the statutory provisions on data protection, in particular for the lawfulness of the disclosure of data to TN and of the data processing.
- (2) TN shall process data only within the scope of the engagement and on the instructions of the Controller, unless a case under Art. 28 (3) (a) GDPR applies. Instructions are initially set out in the Main Contract and may be amended, supplemented or replaced by the Controller in written form or text form (e.g. email) addressed to the contact point designated by TN (individual instruction). Instructions not provided for in the contract shall be treated as a request for a change to the services. Oral instructions shall be confirmed without undue delay in text form or written form.
- (3) TN shall inform the Controller without undue delay if, in TN's opinion, an instruction infringes applicable law, and may suspend its implementation until the Controller confirms or amends it.

Section 4 Obligations of the Processor

- (1) Processing takes place in a Member State of the European Union or in another State party to the Agreement on the European Economic Area. Processing in a third country shall only take place if the conditions of Art. 44 et seq. GDPR are met (adequacy decision or appropriate safeguards, such as EU standard contractual clauses). The Platform and its AI systems are operated in Amazon Web Services data centres in Frankfurt am Main.

- (2) TN shall ensure the security of processing in accordance with Art. 28 (3) (c) and Art. 32 GDPR by means of the technical and organisational measures set out in Annex TOMs. TN also makes Annex TOMs available for download as a separate document. TN may change the measures provided that the level of protection does not fall below the agreed level, and shall regularly review their effectiveness (Art. 32 (1) (d) GDPR).
- (3) Approved codes of conduct pursuant to Art. 40 GDPR or approved certification mechanisms pursuant to Art. 42 GDPR may be submitted as evidence. If TN is unable to submit such evidence, the Controller or a person mandated by it may carry out an audit.
- (4) TN shall structure its internal organisation in such a way that it meets the particular requirements of data protection.
- (5) Inspections by the Controller or by an auditor mandated by it shall take place during normal business hours, without disrupting business operations, after notification with reasonable advance notice (at least 72 hours, on business days). TN may make them conditional on a confidentiality undertaking with regard to the data of other Clients. TN has a right to object to an auditor who is in a direct competitive relationship with TN.
- (6) Paragraph (5) shall apply accordingly to inspections by a data protection authority or other supervisory authority; no confidentiality undertaking is required if the authority is subject to a statutory duty of confidentiality backed by sanctions.
- (7) TN shall notify the Controller without undue delay of any personal data breach affecting the Controller's personal data and of any infringement of data protection provisions by TN, its employees or other third parties, shall take the measures necessary to secure the data and to mitigate adverse effects, and shall coordinate these with the Controller.
- (8) If the Controller's data are jeopardised by attachment or seizure, by insolvency or composition proceedings or by other measures of third parties, TN shall inform the Controller without undue delay and shall inform all parties involved that sovereignty over and ownership of the data lie exclusively with the Controller in its capacity as controller.
- (9) TN shall assist the Controller, insofar as it is able and to the extent necessary, with requests and claims of data subjects under Chapter III GDPR and with the obligations under Art. 33 to 36 GDPR.
- (10) TN shall ensure that the persons authorised to process the data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, also beyond the end of the engagement.
- (11) Contact person for data protection matters at TN: Matthias Maier, Transaction-Network GmbH & Co. KG, Industriepark 312, 78244 Gottmadingen, Tel. +49 7731 16923-23, datenschutz@transaction-network.com. TN's data protection officer is attorney Ulrich Emmert, e|s|b data GmbH, Schockenriedstr. 8A, 70565 Stuttgart, Germany, info@esb-data.de, phone +49 711 46905830.
- (12) TN does not use personal data to train AI systems; Section 11 of the GTC applies.
- (13) After the end of the engagement, TN shall, on request, hand over or delete data, data storage media and other materials, unless statutory retention obligations preclude this; in all other respects, the provisions of the Main Contract on the end of the contract apply (Section 7 of the GTC, Section 6 of the End User Terms of Use, Section 10 (2) of the Freemium Terms of Use). There is no right of retention. Any deletion or destruction going beyond the usual deletion shall be carried out on the basis of a separate order.
- (14) If a data subject brings a claim against the Controller under Art. 82 GDPR, TN shall assist the Controller in defending it insofar as it is able. The Controller shall remunerate such assistance at the rates set out in the Price List; TN shall inform the Controller in advance and on a regular basis of the expected effort.

Section 5 Obligations of the Controller

- (1) The Controller is solely responsible for the lawfulness of the disclosure of data to TN and of the processing within its area of responsibility, and shall comply with its accountability obligation under Art. 5 (2) and Art. 24 (1) GDPR.
- (2) It shall inform TN without undue delay if it discovers errors or irregularities with regard to data protection provisions in the results of the engagement.
- (3) It shall designate to TN a contact person for data protection matters, together with their contact details.

Section 6 Requests from Data Subjects

- (1) If a person exercises a data subject right under Art. 12 et seq. GDPR vis-à-vis TN, TN shall forward the request to the Controller without undue delay and shall assist the Controller to the extent necessary and reasonable.

Section 7 Sub-processors

- (1) The Controller grants TN general authorisation to engage sub-processors. TN shall inform the Controller in advance in text form (e.g. email) of the engagement or replacement of a sub-processor; the Controller may object for good cause relating to data protection.
- (2) Suppliers whose services do not relate directly to the principal service (e.g. telecommunications, postal and transport services, waste disposal, facility management) are not sub-processors.
- (3) TN shall conclude agreements with sub-processors that impose on them the data protection obligations of this Agreement and ensure appropriate data protection and security measures.

Section 8 Special Right of Termination

- (1) The Controller may terminate the Main Contract without observing a notice period if there is a serious breach by TN or by a sub-processor of data protection provisions or of this Agreement.
- (2) A serious breach exists in particular if the agreed technical and organisational measures are not fulfilled to a considerable extent or if the Controller's rights of control are not complied with. In the event of other breaches, the Controller shall set a reasonable period for remedy; if the remedy is not effected in time, the Controller may terminate in accordance with paragraph (1).

Section 9 Liability

- (1) As between the parties, the liability provisions of the Main Contract apply (Section 13 of the GTC, Section 10 of the GTC Consulting, Section 8 of the End User Terms of Use or Section 9 of the Freemium Terms of Use, as applicable). Liability towards data subjects under Art. 82 GDPR remains unaffected.

Section 10 Final Provisions

- (1) In matters of data protection, this Agreement takes precedence over the Main Contract; Section 9 applies to liability.
- (2) Should individual provisions be invalid, the validity of this Agreement and of the Main Contract shall remain unaffected.
- (3) German law applies. The place of jurisdiction is Singen (Hohentwiel), to the extent provided for in the Main Contract.
- (4) This version applies from 1 November 2026 to contracts concluded on or after that day and to End Users and Manufacturers who agree to a version of their terms of use valid from that day. In all other respects, the previous agreement continues to apply to existing contracts.

Annex TOMs: Technical and Organisational Measures

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