

Vertrag zur Auftragsverarbeitung

Vorlage · Stand: 20. September 2026 · tunnl.ch, ein Dienst der xoox ag

Diese Vorlage ist von uns geschrieben und juristisch nicht geprüft. Sie beschreibt wahrheitsgemäss, was tunnl. tut – sie ersetzt aber keine Rechtsberatung. Wer sie unterzeichnen will, lässt sie am besten von der eigenen Rechtsabteilung ansehen; Änderungswünsche nehmen wir entgegen.

1. Parteien

Verantwortliche Stelle (Auftraggeberin): _____

Adresse: _____

Vertreten durch: _____

Auftragsverarbeiterin: xoox ag, Unter Sidhalden 16, 6010 Kriens, Schweiz (UID CHE-210.624.108), Betreiberin des Dienstes tunnl. unter tunnl.ch.

2. Gegenstand und Dauer

Gegenstand ist die Bereitstellung von tunnl.: ein Dienst, mit dem die Auftraggeberin Nachrichten und Dateien Ende-zu-Ende-verschlüsselt übergibt. Der Vertrag gilt, solange die Auftraggeberin tunnl. nutzt, und endet mit der Löschung ihres Kontos.

3. Art, Zweck und Umfang der Bearbeitung

Zweck ist ausschliesslich die vertrauliche Übergabe von Nachrichten und Dateien samt Rückkanal. tunnl. speichert:

- **Verschlüsselte Inhalte** von Nachrichten und Dateien einschliesslich Dateinamen. Die Schlüssel entstehen im Browser und stehen im Teil des Links hinter «#»; sie erreichen den Server nicht. **Die Auftragsverarbeiterin kann die Inhalte nicht entschlüsseln.**
- **Prüfwerte (Hashes)** von Zugangstoken und Zugangsschlüsseln.
- **Technische Angaben ohne Inhalt:** Zeitpunkte von Erstellung, Versand, Abholung und Verfall, Anzahl Nachrichten, Grösse und Frist von Dateien, ob ein Passwort gesetzt ist, Zahl der Fehlversuche.
- **Kontoangaben:** E-Mail-Adresse verschlüsselt und als Prüfwert, gewählte Option, Einstellungen zu Hinweisen.

- **Beim gebrandeten Versand (Option «gotthrd»):** Firmenname, Antwortadresse und Logo im Klartext, weil sie im Mail erscheinen. Adressbuch und Textbausteine liegen verschlüsselt.
- **Beim Mailversand:** Empfängeradresse, Betreff und Begleittext werden im Moment des Versands verarbeitet und nicht gespeichert.

Nicht gespeichert werden: IP-Adressen, Browser-Kennungen, Standortdaten, Cookies zu Werbezwecken.

4. Kategorien betroffener Personen

Mitarbeitende, Kundinnen und Kunden, Lieferanten sowie weitere Personen, an die die Auftraggeberin Nachrichten oder Dateien übergibt oder von denen sie solche empfängt. Welche Personendaten in den verschlüsselten Inhalten stecken, bestimmt allein die Auftraggeberin; der Auftragsverarbeiterin sind sie nicht zugänglich.

5. Weisungen

Die Auftragsverarbeiterin bearbeitet Personendaten nur auf dokumentierte Weisung der Auftraggeberin. Die Nutzung des Dienstes gilt als Weisung. Hält die Auftragsverarbeiterin eine Weisung für rechtswidrig, teilt sie dies mit und darf ihre Ausführung aussetzen.

6. Vertraulichkeit

Alle Personen, die Zugang zu Systemen der Auftragsverarbeiterin haben, sind zur Vertraulichkeit verpflichtet. Die Zahl dieser Personen wird klein gehalten; der Zugang ist mit Zwei-Faktor-Authentifizierung geschützt.

7. Technische und organisatorische Massnahmen

- **Ende-zu-Ende-Verschlüsselung im Browser:** AES-256-GCM, Schlüsselableitung HKDF-SHA-256, bei Passwörtern PBKDF2 mit 600'000 Runden. Dateien werden blockweise verschlüsselt; der Blockindex ist mitgebunden.
- **Server kennt keine Schlüssel.** Zugangstoken liegen nur als Hash vor.
- **Transport:** ausschliesslich HTTPS mit HSTS; strenge Inhalts- und Berechtigungsrichtlinien; keine Fremdskripte, keine externen Schriften, keine Zählwerkzeuge.
- **Anhänge** liegen ausserhalb des Web-Ordners, mit eigener Sperre; jede Datei hat eine Frist und wird nach Ablauf gelöscht.
- **Automatische Löschung:** Konversationen verfallen nach der gewählten Frist; nach zehn Fehlversuchen wird eine Konversation gelöscht. Grabsteine verschwinden nach sieben Tagen.
- **Zugriffsschutz:** Anmeldung per Einmalcode oder Passkey, Sitzungen als Hash gespeichert, «Abmelden auf allen Geräten» im Konto.
- **Sicherheitsprotokoll** ohne IP-Adressen und ohne Inhalte, 90 Tage aufbewahrt.

- **Betrieb** in Rechenzentren in der Schweiz; Zugang nur für wenige berechtigte Personen.

Die Massnahmen entsprechen dem Stand bei Vertragsschluss und dürfen fortentwickelt werden, solange das Schutzniveau nicht sinkt. Der aktuelle Stand steht offen auf tunnl.ch/sicherheit.

8. Unterauftragsverarbeiter

Die Auftraggeberin stimmt folgenden Unterauftragsverarbeitern zu:

- **METANET AG**, Josefstrasse 218, 8005 Zürich, Schweiz – Hosting und Mailversand, Rechenzentren in der Schweiz.

Weitere Unterauftragsverarbeiter werden vorgängig mitgeteilt. Die Auftraggeberin kann binnen 30 Tagen widersprechen; in diesem Fall darf sie den Vertrag kündigen.

9. Ort der Bearbeitung

Schweiz. Eine Bekanntgabe ins Ausland findet nicht statt, ausser die Auftraggeberin oder ihre Empfänger rufen den Dienst aus dem Ausland auf oder die Empfängeradresse liegt bei einem ausländischen Mailanbieter.

10. Unterstützung der Auftraggeberin

Die Auftragsverarbeiterin unterstützt bei Auskunfts-, Berichtigungs- und Löschbegehren, soweit ihr das ohne Kenntnis der Inhalte möglich ist. **Auskunft über Inhalte kann sie nicht erteilen**, weil sie diese nicht entschlüsseln kann; die Auftraggeberin erteilt sie selbst aus ihrem Konto. Löschung einer Konversation ist jederzeit im Konto möglich und wirkt sofort.

11. Meldung von Verletzungen

Wird der Schutz von Personendaten verletzt, meldet die Auftragsverarbeiterin dies der Auftraggeberin unverzüglich, spätestens 48 Stunden nach Kenntnis, mit allen verfügbaren Angaben.

12. Nachweis und Prüfung

Die Auftragsverarbeiterin weist die Einhaltung dieses Vertrags auf Anfrage nach. Eine Prüfung vor Ort ist nach Voranmeldung und während der Geschäftszeiten möglich, höchstens einmal jährlich, soweit sie den Betrieb nicht stört.

13. Löschung nach Vertragsende

Nach Ende des Vertrags werden Konto und zugehörige Daten gelöscht. Verschlüsselte Inhalte verfallen ohnehin nach ihrer Frist. In Sicherungskopien des Hosting-Anbieters können

verschlüsselte Daten bis zum Ablauf der jeweiligen Sicherung verbleiben.

14. Haftung und Recht

Es gilt Schweizer Recht unter Ausschluss des Kollisionsrechts; Gerichtsstand ist Luzern. Soweit die DSGVO auf die Auftraggeberin anwendbar ist, gilt dieser Vertrag als Vereinbarung im Sinne von Art. 28 Abs. 3 DSGVO.

15. Unterschriften

Ort, Datum: _____

Ort, Datum: _____

Für die Auftraggeberin

Für die xoox ag

Name, Funktion

Name, Funktion

Zum Unterschreiben: [als PDF \(DE\)](#) · [PDF \(EN\)](#) · [Datenschutzerklärung](#)