Technische und organisatorische Maßnahmen

Anlage 1 zum Auftragsverarbeitungsvertrag der Founders1 GmbH

Stand: Oktober 2026 · Version 2026-1 · ersetzt die Fassung vom Juni 2024

Vorbemerkung

Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die die Founders1 GmbH (Auftragnehmer) bei der Verarbeitung personenbezogener Daten im Auftrag ihrer Kunden (Auftraggeber) trifft. Sie ist Bestandteil des Auftragsverarbeitungsvertrags.

Der Auftragnehmer ist ein verteilt und mobil arbeitendes Unternehmen. Er unterhält keine eigenen Büro- oder Serverräume und arbeitet papierlos. Die Plattform wird ausschließlich in der Cloud-Infrastruktur von Microsoft Azure betrieben, Region Germany West Central (Frankfurt am Main).

Ein Teil der Maßnahmen, insbesondere die physische Sicherheit der Rechenzentren, wird vom Cloud-Anbieter Microsoft Ireland Operations Ltd erbracht. Diese Maßnahmen sind jeweils als solche gekennzeichnet; ihr Nachweis erfolgt über die Zertifizierungen und die Dokumentation von Microsoft, unter anderem nach ISO/IEC 27001.

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Der Auftragnehmer unterhält keine eigenen Büro- oder Serverräume. Die Zutrittskontrolle zu den Rechenzentren erfolgt durch Microsoft:

- Zutritt nur nach Legitimation mit personenbezogener Zutrittskarte
- Besucher nur nach Voranmeldung und in ständiger Begleitung, ohne Zutritt zu geschützten Bereichen
- Wachschutz rund um die Uhr, Alarmanlage, Schleusensystem, Videoüberwachung und Protokollierung der Zugänge
- Verschlossene Serverracks

1.2 Zugangskontrolle

- Alle Systeme und Anwendungen sind nur nach Authentifizierung zugänglich.
- Persönliche Benutzerkonten für jede Person; Gruppenkonten sind auch für administrative Zugänge nicht zulässig.
- Mehrfaktor-Authentifizierung für Produktivumgebungen, administrative Zugänge, Cloud-Portal, Quellcodeverwaltung, Schlüsselspeicher und E-Mail.
- Passwörter mit mindestens 12 Zeichen in Verbindung mit verpflichtender Mehrfaktor-Authentifizierung; Erstkennwörter nur zur einmaligen Verwendung.
- Automatische Bildschirmsperre nach spätestens 15 Minuten.
- Sofortige Sperrung von Konten und Sitzungen bei Ausscheiden einer Person oder Verlust eines Geräts.

Endgeräte. Die Beschäftigten arbeiten mit eigenen Endgeräten. Dafür gilt:

- Mandatsdaten werden nicht lokal auf Endgeräten gespeichert; die Verarbeitung findet ausschließlich serverseitig statt.
- Zugriffe erfolgen ausschließlich über verschlüsselte Verbindungen.
- Die Beschäftigten verpflichten sich in Textform auf Geräteanforderungen, insbesondere Festplattenverschlüsselung und Bildschirmsperre.
- Beim Ausscheiden bestätigen sie in Textform die Entfernung aller Unternehmensdaten.

1.3 Zugriffskontrolle

- Berechtigungskonzept mit Rollen; Vergabe ausschließlich nach dem Need-to-know-Prinzip.
- Differenzierte Rechte in Anwendungen und Datenbank; Datenbankrechte auf das Notwendige beschränkt.
- Minimale Anzahl administrativer Zugänge.
- Protokollierung von Eingabe, Änderung und Löschung in der Anwendung.
- Überprüfung der Berechtigungen mindestens jährlich, für produktive und administrative Zugänge halbjährlich, jeweils mit Protokoll.
- Verschlüsselung der gespeicherten Daten: Dateispeicher in Azure mit plattformverwalteten Schlüsseln, Datenbank bei MongoDB Atlas mit anbieterverwalteten Schlüsseln.
- Zugriffe von Personal der Cloud-Anbieter: Customer Lockbox für Microsoft Azure ist aktiviert, der Supportzugriff auf die Backend-Infrastruktur von MongoDB Atlas ist gesperrt. Eine Freigabe erteilt nur der Auftragnehmer im Einzelfall, in kritischen Störungs- oder Sicherheitsfällen, zeitlich befristet und protokolliert.

1.4 Trennungskontrolle

- Getrennte Entwicklungs-, Test- und Produktivumgebungen.
- Mandantenfähige Anwendung mit Trennung der Daten je Auftraggeber.
- Dokumente werden je Datensatz in einem eigenen Speicherbereich abgelegt; kein Speicherbereich ist öffentlich zugänglich.
- In Entwicklungs- und Testumgebungen werden ausschließlich erzeugte Testdaten verwendet, keine personenbezogenen Daten aus der Produktion.

1.5 Pseudonymisierung

Zweck der Verarbeitung ist die Identifizierung von Personen und Unternehmen nach dem Geldwäschegesetz; das setzt die Zuordenbarkeit voraus. Pseudonymisierung wird eingesetzt, wo der Zweck es zulässt. Zuordnungsdaten werden dann getrennt und verschlüsselt aufbewahrt.

2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

- Verbindungen zwischen Nutzern und Plattform sind mit TLS 1.2 oder 1.3 verschlüsselt; unverschlüsselte Aufrufe werden auf HTTPS umgeleitet.
- Keine Weitergabe an Dritte außerhalb der vertraglichen Pflichten.
- Mandatsdaten werden nicht in E-Mail-, Chat- oder Ticketsysteme übernommen; Support erfolgt ohne Übermittlung von Mandatsinhalten.
- Einsatz von Unterauftragsverarbeitern ausschließlich nach Anlage 2, jeweils mit Vertrag nach Art. 28 DSGVO.
- Speicherung und Verarbeitung der Mandatsdaten im Europäischen Wirtschaftsraum; die Orte je Dienst nennt Anlage 2. Supportzugriffe der Cloud-Anbieter nur nach Ziffer 1.3 und Ziffer 6.2 AVV.

2.2 Eingabekontrolle

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung über persönliche Benutzerkonten.
- Rechte zur Eingabe, Änderung und Löschung nach dem Berechtigungskonzept.
- Klare Zuständigkeiten für Löschungen und deren Protokollierung.
- Stichproben- und anlassbezogene Auswertung der Protokolle.
- Protokolle enthalten keine Mandatsinhalte und keine personenbezogenen Daten über das zur Zuordnung von Handelnden und Handlung Erforderliche hinaus.

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Sicherungskonzept mit vier Stufen: stündlich (Aufbewahrung 2 Tage), täglich (7 Tage), wöchentlich (4 Wochen) und monatlich (12 Monate).
- Sicherungen sind verschlüsselt und verbleiben im Europäischen Wirtschaftsraum.
- Der Wiederanlauf im Notfall erfolgt ausschließlich in Azure-Regionen im Europäischen Wirtschaftsraum.
- Zugriff auf Sicherungen getrennt vom Zugriff auf die Produktivumgebung.
- Überwachung der Sicherungsläufe; ein fehlgeschlagener Lauf wird als Vorfall behandelt.
- Zielwerte: Wiederherstellungspunkt (RPO) 6 Stunden; Wiederanlaufzeit (RTO) 8 Stunden für Infrastruktur und Datenbank, 12 Stunden für Anwendungen.
- Wiederherstellungstests mindestens jährlich, mit Protokoll.

Durch Microsoft erbracht: Brandmelde- und Löschanlagen, Klimatisierung, unterbrechungsfreie Stromversorgung, redundante Speichersysteme, Schutz vor Hochwasser sowie Überwachung und Alarmierung der Serverräume.

4 Regelmäßige Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d, Art. 25 DSGVO)

- Zentrale Dokumentation aller Regelungen zu Datenschutz und Informationssicherheit.
- Jährliche Überprüfung dieser Maßnahmen und der zugrunde liegenden Richtlinien, mit Protokoll.
- Schulung der Beschäftigten zum Datenschutz bei Eintritt und wiederkehrend.
- Verfahren zur Erkennung, Bewertung, Dokumentation und Nachbereitung von Sicherheitsvorfällen.
- Meldung einer Verletzung des Schutzes personenbezogener Daten an den Auftraggeber unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis.
- Unterstützung des Auftraggebers bei Anfragen betroffener Personen und bei Datenschutz-Folgenabschätzungen.
- Datenschutzfreundliche Voreinstellungen: Es werden nur die für den jeweiligen Zweck erforderlichen Daten verarbeitet.
- Sorgfältige Auswahl und laufende Kontrolle der Unterauftragsverarbeiter.

Nachweise. Der Auftragnehmer verfügt derzeit über keine eigene Zertifizierung. Als Nachweis dienen diese Anlage, das Ergebnis der jährlichen Wirksamkeitsprüfung, die vertraglichen Prüfrechte des Auftraggebers sowie die Zertifizierungen der Unterauftragsverarbeiter.

5 Verarbeitung mit künstlicher Intelligenz

Die Plattform nutzt ein Sprachmodell, um hochgeladene Dokumente auszulesen und Angaben vorzubefüllen.

- **Verarbeitungsweg.** Ausschließlich Azure OpenAI Service der Microsoft Ireland Operations Ltd, in einer auf die EU-Datenzone beschränkten Bereitstellung; die Ressource liegt in der Region Germany West Central. Microsoft verwendet Ein- und Ausgaben nicht zum Training von Modellen. Andere KI-Dienste werden nicht eingesetzt.
- **Isolation und Datenminimierung.** Das Modell erhält je Aufruf nur das jeweilige Dokument. Es hat keinen Zugriff auf Datenbanken, Zugangsdaten oder andere Systeme und behält zwischen Aufrufen nichts. Anweisungen in Dokumenten werden als Inhalt behandelt; Ergebnisse werden auf Manipulationsversuche geprüft.
- **Strukturierte Ergebnisse.** Das Modell liefert nur festgelegte Felder mit Quellenangabe (Seite und Textstelle). Andere Werte werden verworfen.

- **Vorschlag, keine Entscheidung.** KI-Werte sind als solche gekennzeichnet und werden erst nach Bestätigung oder Korrektur durch einen Menschen übernommen. Vorhandene Angaben werden nicht ohne Rückfrage überschrieben. Die KI bewertet keine Personen, vergibt keine Risikoeinstufungen und trifft keine Entscheidungen im Sinne des Art. 22 DSGVO.
- **Gesundheitsdaten.** Ärztliche Unterlagen werden als solche erkannt und abgelegt; ihr Inhalt wird nicht ausgewertet und nicht übernommen.
- **Nachvollziehbarkeit.** Zu jedem Wert werden Quelldokument, Seite, Sicherheit, Status sowie bestätigende Person und Datum gespeichert. Protokolle enthalten keine Dokumentinhalte.
- **Ausfall.** Ist der Dienst nicht erreichbar, bleiben die Dokumente gespeichert; die Angaben werden manuell erfasst.
- **Qualitätssicherung.** Vor jedem Modellwechsel wird das Modell an einem festen Satz fiktiver Musterdokumente mit bekannten Sollwerten geprüft und nur nach bestandener Prüfung eingesetzt.

6 Berufsgeheimnis

Für Auftraggeber, die Berufsgeheimnisträger sind, gilt neben dem Datenschutzrecht § 203 StGB. Ergänzend gilt die Vereinbarung zur beruflichen Verschwiegenheit.

- Verpflichtung aller Personen mit Zugang zu Mandatsdaten zur Verschwiegenheit in Textform vor Aufnahme der Tätigkeit, mit Belehrung über die Strafbarkeit.
- Entsprechende Verpflichtung der Unterauftragsverarbeiter, die Mandatsdaten erhalten, einschließlich der Verpflichtung ihrer eigenen Unterauftragnehmer. Microsoft und MongoDB bieten eine gesonderte Verpflichtung nach § 203 StGB nicht an; der Zugriff ihres Personals ist nach Ziffer 1.3 gesperrt und nur nach Freigabe möglich.
- Führung eines Verpflichtungsregisters, dessen Stand dem Auftraggeber auf Verlangen offengelegt wird.

7 Änderungen

Der Auftragnehmer entwickelt die Maßnahmen fort. Das Schutzniveau dieser Anlage wird dabei nicht unterschritten. Wesentliche Änderungen werden dem Auftraggeber vorab in Textform angezeigt.

Founders1 GmbH · Sitz Berlin, Amtsgericht Charlottenburg, HRB 234373 B · Geschäftsanschrift Berger Straße 224, 60385 Frankfurt am Main