ANLAGE I
TECHNISCH-ORGANISATORISCHE MAßNAHMEN (TOMS) GEM. ART. 32 DSGVO I.V.M. § 5 DES AVV

Auftragsverarbeiter: Robert Daniel, Osakaallee 18, 20457 Hamburg Stand: November 2026

1. Zutrittskontrolle Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen verwehrt. Die Tätigkeit erfolgt in privaten Räumlichkeiten mit kontrolliertem Zutritt. Dritte haben keinen unbeaufsichtigten Zugang zu Arbeitsmitteln.

2. Zugangskontrolle Systeme sind durch starke Passwörter und automatische Bildschirmsperre gesichert. Alle Endgeräte sind mit einer vollständigen Festplattenverschlüsselung gesichert (macOS: FileVault / Windows: BitLocker). Der Zugang zu cloudbasierten Diensten erfolgt ausschließlich mit Zwei-Faktor-Authentifizierung (2FA).

3. Zugriffskontrolle Zugriff auf personenbezogene Daten des Verantwortlichen erfolgt ausschließlich im Rahmen des vertraglich definierten Auftrags. Eine Weitergabe an Dritte findet nicht statt. Subunternehmen werden nur mit ausdrücklicher schriftlicher Zustimmung des Verantwortlichen eingesetzt (vgl. § 8 AVV).

4. Weitergabekontrolle Die Übertragung personenbezogener Daten erfolgt ausschließlich über verschlüsselte Verbindungen (TLS/HTTPS). Eine Übermittlung per unverschlüsselter E-Mail findet nicht statt. Dokumente mit personenbezogenem Inhalt werden nicht über nicht-autorisierte Dienste geteilt.

5. Eingabekontrolle Verarbeitungstätigkeiten sind nachvollziehbar dokumentiert. Änderungen an Datenbeständen des Verantwortlichen sind rückverfolgbar. Eine unbefugte Eingabe, Veränderung oder Löschung von Daten wird durch Zugriffsbeschränkungen verhindert.

6. Auftragskontrolle Daten des Verantwortlichen werden ausschließlich gemäß dessen dokumentierten Weisungen verarbeitet. Eine Verarbeitung zu eigenen Zwecken findet nicht statt.

7. Verfügbarkeitskontrolle Arbeitsmittel sind durch regelmäßige Datensicherung geschützt. Backups werden verschlüsselt auf einem separaten Medium oder einem DSGVO-konformen Cloud-Dienst gespeichert. Im Falle eines Datenverlusts wird der Verantwortliche unverzüglich informiert.

8. Trennungskontrolle Daten verschiedener Auftraggeber werden organisatorisch und technisch getrennt verarbeitet. Eine Vermischung von Mandantendaten findet nicht statt. Je Auftraggeber werden separate Verzeichnisse und Zugänge geführt.

9. Einsatz von KI-Tools und cloudbasierten Diensten Soweit im Rahmen der Auftragserfüllung KI-gestützte Werkzeuge eingesetzt werden, erfolgt dies ausschließlich über Dienste mit nachgewiesener DSGVO-Konformität, EU-Datenresidenz und vorliegendem Auftragsverarbeitungsvertrag. Aktuell eingesetzt: LangDock (ISO 27001, SOC 2 Type II, AVV nach deutschem Recht, EU-Hosting). Der Einsatz weiterer Dienste mit Personenbezug erfolgt nur nach vorheriger Zustimmung des Verantwortlichen.

10. Vertraulichkeit und Mitarbeiterverpflichtung Der Auftragsverarbeiter ist zur Vertraulichkeit verpflichtet. Da keine weiteren Mitarbeitenden eingesetzt werden, entfällt eine gesonderte Mitarbeiterverpflichtung. Subunternehmen werden, sofern eingesetzt, schriftlich zur Einhaltung gleichwertiger Datenschutzstandards verpflichtet.

11. Löschung und Rückgabe Nach Beendigung des Auftrags werden alle Daten des Verantwortlichen vollständig gelöscht oder zurückgegeben. Dies umfasst lokale Kopien, Cloud-Speicher und Verarbeitungsergebnisse. Ein Löschprotokoll wird auf Anforderung vorgelegt.