Anlage 1 zum AVV: Technische und organisatorische Maßnahmen

Maßnahmen nach Art. 32 DSGVO zum Auftragsverarbeitungsvertrag (SV-AVV-1.0). Bestandteil des Vertrags; keine gesonderte Unterschrift erforderlich.

Diese Anlage beschreibt die von Sunventory zum Stand 12.06.2026 getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus (Art. 32 DSGVO). Die Maßnahmen werden gemäß § 5 des Auftragsverarbeitungsvertrags (SV-AVV-1.0) fortgeschrieben; das vereinbarte Sicherheitsniveau darf dabei nicht unterschritten werden.

> Hinweis zur Einordnung: Die Verarbeitung erfolgt ausschließlich in Rechenzentren des Hosting-Anbieters IONOS SE in Deutschland. Die Rechenzentren des Hosting-Anbieters sind nach ISO 27001 zertifiziert. Sunventory selbst hält keine eigene Zertifizierung.

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

1.1 Zutrittskontrolle

- Betrieb von Backend, Datenbank und Website ausschließlich in Rechenzentren des Hosting-Anbieters IONOS SE in Deutschland; die Rechenzentren sind nach ISO 27001 zertifiziert.
- Die physische Zutrittskontrolle zu den Rechenzentren obliegt dem Hosting-Anbieter und ist Gegenstand des mit ihm geschlossenen Auftragsverarbeitungsvertrags (vgl. Anlage 2: Unterauftragsverarbeiter (SV-SUB-1.0)).

1.2 Zugangskontrolle

- Authentifizierung der Nutzer gegenüber dem Backend mittels JWT (JSON Web Token).
- Rollenbasierte Rechtevergabe (Rollen: Bauleitung, Einkauf, Asset Management, Operativ).
- Zwei-Faktor-Authentisierung für administrative Zugänge von Sunventory.
- Sichere Token-Speicherung auf den Endgeräten: iOS-Keychain bzw. Android EncryptedSharedPreferences (AES-256, Schlüssel im Android Keystore).

1.3 Zugriffs- und Trennungskontrolle

- Mandantentrennung auf Anwendungs- und Datenbankebene (mandantenfähige Architektur); Daten verschiedener Kunden werden logisch getrennt verarbeitet.
- Zugriff auf personenbezogene Daten nur im Rahmen der rollenbasierten Berechtigungen.
- Prinzip der Datensparsamkeit: Es werden nur die für den Leistungszweck erforderlichen Daten verarbeitet; keine Analyse-, Werbe- oder Tracking-SDKs Dritter in den Apps, keine Werbe-IDs.

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

- TLS-Transportverschlüsselung für die Datenübertragung zwischen Clients (Web, iOS, Android) und Backend.
- Protokollierung administrativer Zugriffe.
- Server-Logfiles werden maximal 14 Tage vorgehalten.

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

- Tägliche Backups der Datenbank.
- Regelmäßige Wiederherstellungstests der Backups.
- Automatisches Überschreiben der Backups spätestens nach 35 Tagen.
- Betrieb in deutschen Rechenzentren des Hosting-Anbieters; keine Verarbeitung außerhalb Deutschlands, keine Drittlandübermittlung.

4. Besonderheit: On-Device-Texterkennung (OCR)

- Die Texterkennung (OCR) der Lieferscheine läuft ausschließlich on-device auf dem Endgerät des Nutzers (iOS: Apple Vision Framework; Android: Google ML Kit).
- Zum Zweck der Texterkennung werden keine Bilder und keine erkannten Texte an Dritte oder an KI-Cloud-Dienste übertragen.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Jährliche Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen.
- Anlassbezogene Anpassung, insbesondere bei Änderungen der Verarbeitung, bei Sicherheitsvorfällen und bei neuen Erkenntnissen zum Stand der Technik.
- Fortschreibung gemäß § 5 des Auftragsverarbeitungsvertrags (SV-AVV-1.0); das Sicherheitsniveau darf nicht unterschritten werden.

6. Organisatorische Maßnahmen

- Verpflichtung aller zur Verarbeitung befugten Personen auf Vertraulichkeit (Art. 28 Abs. 3 UAbs. 1 lit. b, Art. 29 DSGVO).
- Löschkonzept mit definierten Lösch- und Aufbewahrungsfristen; Umsetzung der Lösch- und Rückgabepflichten gemäß § 10 des Auftragsverarbeitungsvertrags (SV-AVV-1.0).
- Dokumentierter Datenpannen-Prozess einschließlich Verletzungsregister; Meldung an den Kunden unverzüglich, spätestens 24 Stunden nach Kenntnis, gemäß § 8 des Auftragsverarbeitungsvertrags (SV-AVV-1.0).