AVV Anlage 1 -- Technische und Organisatorische Maßnahmen (TOMs)

gemäß Art. 32 DSGVO

Anlage zum Rahmen-Auftragsverarbeitungsvertrag der **EXT IT GmbH**

Vorbemerkung

Die EXT IT GmbH betreibt eine **hybride Infrastruktur** bestehend aus einem Dedicated Server in einem Rechenzentrum innerhalb der EU (Deutschland) sowie EU-basierten Cloud-Diensten. Der Rechenzentrumsbetreiber unterhält ein nach **ISO/IEC 27001 zertifiziertes Informationssicherheits-Managementsystem** für die Bereitstellung und Verwaltung von Rechenzentrumsdiensten; der Geltungsbereich umfasst die genutzten Standorte. Der Zertifikatsnachweis wird dem Auftraggeber auf Anforderung vorgelegt. Der Hosting-Anbieter gewährleistet die **physische Sicherheit** des Rechenzentrums; er erhält keinen Zugriff auf die verarbeiteten Daten. Der Auftragnehmer trägt die Verantwortung für die **logische und softwareseitige Sicherheit** (Betriebssysteme, Patches, Firewall-Konfiguration, Dienste und Anwendungen) auf dem Dedicated Server nach Maßgabe dieser TOMs. Ergänzend betreibt der Auftragnehmer am Standort Hannover in eigenen, zugangsgesicherten Geschäftsräumen eigene Infrastruktur, auf der die **verschlüsselte Offsite-Datensicherung** vorgehalten wird; Dritte sind hieran nicht beteiligt. Die Details zu eingesetzten Unterauftragsverarbeitern ergeben sich aus Anlage 3.

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

1.0 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- **Daten in Transit:** Durchgängige Transportverschlüsselung auf allen Kanälen gemäß jeweils aktueller BSI-Empfehlung (TR-02102): TLS für Web-, E-Mail- und Cloud-Zugriffe, moderne VPN-Kryptographie mit Perfect Forward Secrecy für Remote-Zugriffe, SSH mit Key-Authentifizierung für Server-Administration
- **Backups:** Offsite- und Langzeitsicherungen werden grundsätzlich mit AES-256 verschlüsselt; das Schlüsselmaterial wird getrennt von den Sicherungsdaten verwahrt und ist auf einen namentlich festgelegten Personenkreis beschränkt
- **Cloud-Dienste:** Verschlüsselung at Rest (AES-256) auf Ebene der eingesetzten EU-Cloud-Plattformen
- **Endgeräte:** Vollständige Geräteverschlüsselung auf dienstlich bereitgestellten Notebooks und mobilen Geräten
- **Produktivsystem:** Die Datenträger des Produktivsystems sind auf Blockebene verschlüsselt. Die kryptographischen Schlüssel werden ausschließlich vom Auftragnehmer verwaltet und **nicht beim Hosting-Anbieter hinterlegt**; ein Auslesen der Daten über den physischen Zugang zur Hardware ist damit ausgeschlossen
- **Produktivdaten:** Ergänzende kryptographische und organisatorische Schutzmaßnahmen werden risikobasiert eingesetzt; dies umfasst insbesondere Offsite-Backups in AES-256-Verschlüsselung mit getrennter Schlüsselverwahrung, Cloud-Dienste mit Verschlüsselung at Rest auf AES-256-Niveau, physische Zutrittskontrolle im Rechenzentrum des Hosting-Anbieters, strenge logische Zugriffskontrolle (phishing-resistente MFA, VPN-Pflicht, Least-Privilege-Berechtigungen), System-Hardening sowie kontinuierliches Monitoring.
- **Pseudonymisierung:** Pseudonymisierung wird grundsätzlich eingesetzt, wo der Verarbeitungszweck dies zulässt (z.B. Pseudonym-IDs in Monitoring-Systemen statt Klarnamen, sofern technisch praktikabel)

- **Testdaten:** Es werden ausschließlich nicht-personenbezogene oder anonymisierte Daten verwendet, siehe 5.3
- **Schlüsselmanagement:** Kryptographische Schlüssel werden getrennt von den verschlüsselten Daten verwahrt; privilegierter Zugriff ist auf das erforderliche Minimum beschränkt

1.1 Zutrittskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren:

Rechenzentrum (durch Hosting-Anbieter, siehe Anlage 3):

- Betrieb durch einen Anbieter mit nach ISO/IEC 27001 zertifiziertem Informationssicherheits-Managementsystem (siehe Vorbemerkung)
- Umfriedetes Betriebsgelände, Zutrittszonenkonzept
- Zutrittskontrollsystem, Sicherheitsschlösser, dokumentierte Schlüsselregelung
- Videoüberwachung der Eingänge
- Besucherausweise, Begleitpflicht und Besucherprotokoll

Eigene Infrastruktur am Standort Hannover (Offsite-Datensicherung):

- Unterbringung in eigenen Geschäftsräumen des Auftragnehmers; kein Zugang Dritter
- Sicherungssysteme in einem verschlossenen, baulich abgetrennten Serverschrank
- Schlüsselgewalt ausschließlich beim Auftragnehmer; Zutritt nur namentlich autorisierte Personen
- Getrennter Betrieb von der übrigen Büroumgebung
- Sicherungsdaten ausschließlich verschlüsselt vorgehalten (siehe 1.0 und 3.1)

Arbeitsplatz:

- Zugangskontrolle zum Arbeitsplatz (personalisierte Zugangsmittel)
- Clean-Desk-Policy (keine Kundendaten auf physischen Arbeitsplätzen)
- Sichere Verwahrung mobiler Dienstgeräte
- Besucherregelung (Begleitung, kein unbeaufsichtigter Zugang)
- Wegschließen vertraulicher Papierdokumente

1.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte Datenverarbeitungssysteme nutzen können:

- Phishing-resistente Multi-Faktor-Authentifizierung für alle Benutzer
- Passwort-Policy nach aktueller BSI-Empfehlung (Grundschutz)
- Erhöhte Passwort-Anforderungen für privilegierte Konten nach BSI-Grundschutz-Empfehlung
- Zentraler, Ende-zu-Ende-verschlüsselter Passwort-Manager
- VPN-Pflicht für alle Fernzugriffe (Zero-Trust-Architektur)
- Administrative Zugänge ausschließlich über autorisierte Wege; schlüssel- oder zertifikatsbasierte Authentifizierung
- Automatische Bildschirmsperre nach angemessener Inaktivitätsdauer
- Geräteverschlüsselung auf allen Endgeräten
- Account-Lockout nach festgelegten Fehlversuchen mit Benachrichtigung bei sicherheitsrelevanten Ereignissen
- Risikobasierte Conditional-Access-Policies (standort-, geräte- und risikobasiert)
- Technisch erzwungene Änderung von Initialpasswörtern; Verbot der Passwortweitergabe
- Kennworthistorie zur Vermeidung von Wiederverwendung

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass Berechtigte nur auf die Daten zugreifen können, für die sie berechtigt sind:

- Rollen- und rechtebasiertes Berechtigungskonzept (Least-Privilege-Prinzip)
- Strikte Trennung privilegierter und Standard-Konten
- Namentlich festgelegte Administratoren mit privilegiertem Zugang
- Regelmäßige Berechtigungsreviews
- Sofortiger Berechtigungsentzug bei Austritt/Aufgabenwechsel
- Zentrale Zugriffsprotokolle (Audit-Logs) in allen relevanten Systemen
- Zentrales Identitätsmanagement über Identity-Provider
- Server-Hardening nach Industriestandard (CIS/BSI) über Configuration Management
- Gewährleistung der fachlichen und persönlichen Eignung von Administratoren durch Auswahl, Schulung und regelmäßige Überprüfung
- Zentrale Protokollierung und Alarmierung verdächtiger Aktivitäten
- Endpoint-Schutz auf allen Servern und Administrations-Endpoints

1.4 Weitergabekontrolle / Übertragungskontrolle

Maßnahmen, die die Integrität und Vertraulichkeit bei der Übertragung personenbezogener Daten gewährleisten:

- Durchgängige Transportverschlüsselung (TLS, VPN, SSH) nach Maßgabe der in §1.0 genannten BSI-Empfehlung
- Verschlüsselung at Rest (AES-256) für Cloud-Dienste und Offsite-Backups
- Ende-zu-Ende-verschlüsselte VPN-Verbindungen für alle internen Verbindungen
- E-Mail-Kommunikation über die eingesetzte EU-Cloud-Plattform mit TLS-Transportverschlüsselung; eine inhaltsseitige Ende-zu-Ende-Verschlüsselung (S/MIME/PGP) ist nicht standardmäßig eingerichtet und kann projektspezifisch nach gesonderter Vereinbarung bereitgestellt werden
- Host-Firewall mit Deny-all-Standardregel auf allen Servern; vorgelagerte Perimeter-Firewall
- Vertragliche Geheimhaltungsvereinbarungen mit allen Dienstleistern und Unterauftragnehmern
- Datenaustausch nur über verschlüsselte Plattformen
- Verpflichtung zum Schutz von Datenträgern gegen Verlust und Beschädigung
- Etabliertes Incident-Response-System für Datenschutzverletzungen

1.5 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Logische Mandantentrennung pro Kunde in allen Systemen
- Separate Tenants für Kundendaten
- Pro-Kunde-Trennung bei gehosteten Anwendungen
- Netzwerksegmentierung durch separate virtuelle Netzwerke und Firewall-Regeln
- Zugriffsbasierte Trennung (Mitarbeiter sehen nur Daten zugewiesener Kunden)

---

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

2.1 Eingabekontrolle

Maßnahmen, die nachvollziehbar machen, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt wurden:

- Zentrale Protokollierung mit Korrelation aller Sicherheitsereignisse
- Zentralisierte Syslog-Erfassung mit angemessener Aufbewahrungsfrist
- Audit-Logs für alle Cloud-Dienste und Identitätssysteme (Sign-in- und Audit-Logs)
- Integritätsüberwachung sicherheitsrelevanter Dateien auf allen Servern
- Versionierung aller Dokumente
- Vollständige Login-/Logout-Protokollierung

- Protokollierung aller Eingabe-, Änderungs- und Löschzugriffe
- Automatisierte Reports über Verarbeitungsaktivitäten
- Anomalieerkennung für verdächtige Aktivitäten
- Umfassende Audit-Protokollierung relevanter Sicherheitsereignisse

2.2 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten nur gemäß den Weisungen des Auftraggebers verarbeitet werden:

- Auftragsverarbeitungsverträge nach Art. 28 DSGVO mit den eingesetzten Unterauftragnehmern; der jeweils aktuelle Stand je Unterauftragnehmer ist in Anlage 3 ausgewiesen
- Dokumentierte Weisungen über Ticketsystem
- Verpflichtung aller Mitarbeiter auf das Datengeheimnis
- Einweisung der mit dem Auftrag betrauten Mitarbeiter in die Datenschutzanforderungen
- Dokumentation aller Weisungen des Auftraggebers
- Jährliche Überprüfung der Unterauftragnehmer auf Compliance
- Risikobasierte Auswahl von Unterauftragnehmern
- Verbot der Einbindung von Unterauftragnehmern in unsicheren Drittstaaten

---

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

3.1 Verfügbarkeits- und Wiederherstellungskontrolle

Maßnahmen zum Schutz gegen zufällige Zerstörung oder Verlust sowie zur raschen Wiederherstellung bei physischen oder technischen Zwischenfällen:

- Regelmäßige Datensicherungen (lokal auf dem Dedicated Server sowie Offsite-Backup an einem separaten Standort des Auftragnehmers)
- Offsite-Backups AES-256 verschlüsselt; Schlüsselmaterial getrennt von den Sicherungsdaten verwahrt
- Dokumentierte Wiederherstellungsverfahren mit regelmäßigen Restore-Tests
- USV und Notstromversorgung durch das Rechenzentrum des Hosting-Anbieters
- Monitoring und Alerting: zentrale Protokollierung mit Benachrichtigung bei sicherheitsrelevanten Ereignissen
- Host-Firewall mit Default-Deny-Policy auf allen Servern und dedizierte VM-Firewall
- Endpoint-Schutz auf allen Servern und Administrations-Endpoints
- Spam- und Malware-Filter für E-Mail-Kommunikation
- Automatische Sicherheitsupdates über Configuration Management
- Rauch- und Brandmelder am Arbeitsplatz
- Brandfrüherkennung und Löschanlage im Rechenzentrum des Hosting-Anbieters

---

4. Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen zur Aufrechterhaltung der Verarbeitung bei Störungen und hoher Belastung:

- Virtualisierung aller Dienste (schnelle Wiederherstellung einzelner VMs/Container)
- Redundante Datensicherung (lokal + Offsite)
- Automatisierte Systemkonfiguration via Configuration Management (schneller Neuaufbau von Systemen)
- Von den Anwendungssystemen getrennte Firewall-Instanz zur Isolation von Netzwerkstörungen
- DDoS-Grundschutz durch den Rechenzentrumsanbieter

---

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

5.1 Datenschutzorganisation

- Datenschutzverantwortung direkt bei der Geschäftsführung
- Jährliche Risikobewertung aller Verarbeitungstätigkeiten und IT-Systeme
- Jährlicher Überprüfungszyklus aller Richtlinien und dieser TOMs (nächste Überprüfung siehe Metadaten)
- Datenschutzanforderungen in Toolauswahl und Servicedesign integriert
- Verfahren zur Beobachtung der Entwicklung rechtlicher und technischer Datenschutzanforderungen
- Anlassbezogene Überprüfung bei wesentlichen Änderungen der Infrastruktur, Bedrohungslage oder Rechtslage

5.2 Schulung und Awareness

- Regelmäßige Awareness-Maßnahmen zu Datenschutz und Informationssicherheit
- Einweisung neuer Mitarbeiter in Datenschutz- und Sicherheitsanforderungen

5.3 Privacy by Design und Default

- Verwendung nicht-personenbezogener Testdaten bei der Entwicklung
- Verschlüsselung als Standard bei allen Übertragungswegen sowie bei Backups und Cloud-Diensten
- Ausschließlich lokale KI-Systeme; keine Kundendaten an externe KI-Anbieter

5.4 Weitergabe-Dokumentation

- Protokollierung aller Datenabrufe
- Regelmäßige Auswertung der Zugriffs- und Weitergabeprotokolle
- Anomalieerkennung bei Datenweitergaben
- Risikobasierte Auswahl von Dienstleistern

5.5 Technische Wirksamkeitsprüfung

- Regelmäßige Schwachstellenscans und Auswertung der Ergebnisse
- Abweichungserkennung gegenüber Soll-Konfiguration auf allen Servern
- Auswertung zentraler Protokolle, Integritäts- und Audit-Ereignisse
- Penetrations- oder Sicherheitsprüfungen anlassbezogen und im Rahmen der jährlichen Risikobewertung

---

6. Mobiles Arbeiten und Remote-Zugriff

Maßnahmen zur Gewährleistung des Datenschutzes und der Informationssicherheit bei mobilem Arbeiten:

- Mobiles Arbeiten (Home-Office, Remote) ist gestattet, sofern das Sicherheitsniveau der vorstehenden TOMs eingehalten wird
- Sämtliche Fernzugriffe auf Unternehmenssysteme und Kundendaten erfolgen ausschließlich über verschlüsselte VPN-Verbindungen
- Für die Datenverarbeitung dürfen ausschließlich Endgeräte eingesetzt werden, die zentral verwaltet und mit aktuellen Sicherheitsrichtlinien konfiguriert sind; dies gilt auch für privat beschaffte Endgeräte, die nur nach Aufnahme in die zentrale Geräteverwaltung genutzt werden dürfen
- Anweisung zur Nutzung von Sichtschutzfolien an öffentlichen Orten; Verbot der Verarbeitung vertraulicher Daten in öffentlich einsehbaren Bereichen

- Nutzung offener/ungesicherter WLAN-Netze nur in Verbindung mit aktivem VPN gestattet
- Endgeräte sind bei Nichtbenutzung zu sperren und sicher aufzubewahren; eine lokale Speicherung von Kundendaten auf privat beschafften Endgeräten ist untersagt
- Vertrauliche Dokumente dürfen im mobilen Arbeiten nicht ausgedruckt werden, es sei denn, eine sichere Vernichtung ist gewährleistet

---

7. NIS2-Konformität (§ 30 BSIG n.F.)

Soweit der Auftragnehmer oder der Auftraggeber den Anforderungen des NIS2-Umsetzungsgesetzes unterliegt, werden folgende ergänzende Maßnahmen umgesetzt:

7.1 Risikomanagement (§ 30 Abs. 2 Nr. 1 BSIG n.F.)

- Jährliche Risikobewertung aller Verarbeitungstätigkeiten und IT-Systeme
- Systematische Bewertung der Bedrohungslage
- Regelmäßiger Überprüfungszyklus aller sicherheitsrelevanten Richtlinien

7.2 Bewältigung von Sicherheitsvorfällen (§ 30 Abs. 2 Nr. 2 BSIG n.F.)

- Meldepflicht an Auftraggeber gemäß §14 Abs. 6 lit. b AVV-Rahmenvertrag: Erstmeldung unverzüglich, bei NIS2-verpflichteten Auftraggebern in der Regel innerhalb 24 Stunden, sonst innerhalb 48 Stunden; Detailmeldung in der Regel innerhalb 72 Stunden (§ 32 BSIG n.F.)
- Nachbereitung und Lessons-Learned-Prozess nach Sicherheitsvorfällen
- Zentrale Erkennung und Korrelation von Sicherheitsereignissen
- Benachrichtigung bei sicherheitsrelevanten Alerts

7.3 Aufrechterhaltung des Betriebs (§ 30 Abs. 2 Nr. 3 BSIG n.F.)

- Regelmäßige Datensicherungen (lokal + Offsite an separatem Standort)
- Offsite-Backups AES-256 verschlüsselt
- Virtualisierung aller Dienste ermöglicht schnelle Wiederherstellung einzelner Systeme
- Automatisiertes Configuration Management für schnellen Neuaufbau

7.4 Sicherheit der Lieferkette (§ 30 Abs. 2 Nr. 4 BSIG n.F.)

- Risikobasierte Auswahl und regelmäßige Überprüfung von Unterauftragsverarbeitern
- Vertragliche Verpflichtung aller Unterauftragsverarbeiter auf Sicherheitsanforderungen
- Zentrale Dokumentation aller Unterauftragsverarbeiter (Anlage 3)
- Jährliche Überprüfung der Unterauftragnehmer auf Compliance

7.5 Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung (§ 30 Abs. 2 Nr. 5 BSIG n.F.)

- Automatische Sicherheitsupdates über Configuration Management
- Server-Hardening nach Industriestandard (CIS/BSI)
- Vulnerability Management mit regelmäßigen Scans
- Configuration Management mit Abweichungserkennung

7.6 Schulung und Awareness (§ 30 Abs. 2 Nr. 8 BSIG n.F.)

- Jährliche Pflichtschulung Datenschutz und Informationssicherheit für alle Mitarbeiter
- Einweisung neuer Mitarbeiter in Datenschutz- und Sicherheitsanforderungen
- Sensibilisierung für aktuelle Bedrohungen (Phishing, Social Engineering)

7.7 Zugangskontrolle und Asset-Management (§ 30 Abs. 2 Nr. 9 BSIG n.F.)

- Multi-Faktor-Authentifizierung (MFA) für alle Benutzer
- Zero-Trust-Architektur mit VPN-Pflicht
- Rollen- und rechtebasiertes Berechtigungskonzept (Least Privilege)
- Zentrales Asset-Management und Inventarisierung

Stand: 2026-08-12