snapAddy

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

Im Zuge der Auftragsverarbeitung ergreift der Auftragnehmer folgende technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus.

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

a. Zutrittskontrolle

Maßnahmen zur Verhinderung des Zutritts Unbefugter zu Datenverarbeitungsanlagen:

- Elektronische Zutrittskontrolle im gesamten Gebäudekomplex
- Zutritt mittels zentraler Schließanlage für berechtigte Personen
- Verwaltung individueller Zutrittsprofile (zeitlich und räumlich eingeschränkt)
- Zutrittskontrolle zu Hosting-Systemen erfolgt durch den Subdienstleister (AWS) gemäß dessen zertifizierten Sicherheitsmaßnahmen (u. a. ISO 27001, SOC 2)

b. Zugangskontrolle

Maßnahmen zur Verhinderung der Nutzung von IT-Systemen durch Unbefugte:

- Einsatz von Firewall-Systemen, Anti-Malware-Lösungen und Proxy-Systemen
- Einheitliche Passwortrichtlinie:
  - mindestens 12 Zeichen
  - Kombination aus Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen
  - keine Wiederverwendung von Passwörtern
  - verpflichtende Nutzung eines Passwortmanagers
- Multi-Faktor-Authentifizierung (MFA):
  - verpflichtend für privilegierte Zugänge und kritische Systeme
  - Umsetzung ausschließlich über sichere Verfahren (z. B. TOTP-basierte Authenticator-Apps)
  - SMS-basierte Verfahren sind nicht zugelassen
- Mobile Geräte sind durch PIN (mind. 6-stellig) oder biometrische Verfahren geschützt
- Zugriff ausschließlich über verschlüsselte Verbindungen (TLS 1.2 / TLS 1.3 gemäß Stand der Technik, z. B. BSI TR-02102-2)

c. Zugriffskontrolle

Maßnahmen zur Sicherstellung, dass Berechtigte nur auf erforderliche Daten zugreifen:

- Rollenbasierte Zugriffskontrolle (RBAC) nach dem Least-Privilege-Prinzip
- „Deny by Default"-Ansatz (keine Berechtigung ohne explizite Freigabe)
- Rechtevergabe und -prüfung erfolgen regelmäßig (mind. jährlich, bei kritischen Systemen häufiger)
- Zugriff nur über personalisierte Benutzerkonten mit MFA
- Verschlüsselung von Daten und Datenträgern (AES-256)
- Kontinuierliches Monitoring der Systeme zur Erkennung unberechtigter Zugriffe
- Sicherheitslücken werden zeitnah identifiziert und behoben

d. Pseudonymisierung

Maßnahmen zur Trennung von Identifikationsmerkmalen:

- Einsatz von Pseudonymisierung, sofern technisch und organisatorisch sinnvoll (z. B. Tokenisierung)
- Trennung von Identifikationsdaten und Fachdaten
- Separate und geschützte Aufbewahrung der Zuordnungsinformationen
- Klare Abgrenzung zur Verschlüsselung:
  - Verschlüsselung (z. B. AES-256) dient dem Schutz der Vertraulichkeit
  - Pseudonymisierung reduziert die direkte Personenbeziehbarkeit

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

a. Weitergabekontrolle

Maßnahmen zur Sicherstellung sicherer Datenübertragung:

- Datenübertragung ausschließlich verschlüsselt (TLS 1.2 / TLS 1.3)
- Verwendung sicherer Cipher Suites gemäß Stand der Technik
- Verschlüsselung von Datenträgern
- Berechtigungskonzept für Datenübermittlung, -änderung und -löschung
- Vertragliche Verpflichtung aller Mitarbeitenden auf Vertraulichkeit
- Zugriffsbeschränkungen beim Hosting-Dienstleister durch technische und organisatorische Maßnahmen (z. B. Verschlüsselung, Netzwerksegmentierung, Zertifizierungen)

b. Eingabekontrolle

Maßnahmen zur Nachvollziehbarkeit von Datenverarbeitung:

- Protokollierung aller Eingaben, Änderungen und Löschungen personenbezogener Daten
- Zuordnung zu individuellen Benutzerkonten
- Zugriff auf Protokolle nur für berechtigtes Personal

c. Logging und Monitoring

Maßnahmen zur Überwachung und Erkennung sicherheitsrelevanter Ereignisse:

- Zentrale Erfassung von Log-Daten (z. B. System-, Audit- und Cloud-Logs)
- Definition von Verantwortlichkeiten, Speicherorten und Aufbewahrungsfristen
- Regelmäßige Auswertung der Logs
- Automatisierte Erkennung von Anomalien
- Übergabe sicherheitsrelevanter Ereignisse an Incident-Management-Prozesse

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

a. Verfügbarkeitskontrolle

Maßnahmen zum Schutz vor Datenverlust:

- Dokumentiertes Backup- und Recovery-Konzept
- Regelmäßige Datensicherungen (z. B. tägliche Backups)

- Definierte Aufbewahrungsfristen (z. B. 30 Tage)
- Regelmäßige Wiederherstellungstests (mind. jährlich)
- Zielparameter:
  - RPO (Recovery Point Objective): max. 24 Stunden
  - RTO (Recovery Time Objective): max. 1 Geschäftstag
- Verschlüsselte Speicherung von Backups (AES-256)
- Nutzung hochverfügbarer Rechenzentren (AWS) mit physischer Absicherung (z. B. Brand- und Umweltschutz)

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

a. Auftragskontrolle

- Verarbeitung personenbezogener Daten ausschließlich gemäß Art. 28 DSGVO und vertraglicher Weisung
- Kontroll- und Auditrechte des Auftraggebers werden unterstützt
- Nachweisführung über getroffene Maßnahmen
- Absicherung von Subdienstleistern durch vertragliche Regelungen und Zertifizierungen

b. Trennungsgebot

- Logische Trennung von Daten unterschiedlicher Mandanten
- Trennung von Test- und Produktivumgebungen
- Keine Nutzung von Echtdaten in Testsystemen

c. Datensicherheitsmanagement

- Betrieb eines Informationssicherheitsmanagementsystems (ISMS), z. B. nach ISO 27001
- Regelmäßige Überprüfung und Weiterentwicklung der Sicherheitsmaßnahmen
- Versionierung und Aktualisierung der TOM-Dokumentation

d. Datenschutzfreundliche Voreinstellungen (Privacy by Default)

- Umsetzung des „Deny by Default“-Prinzips
- Minimalprinzip bei Datenerhebung und -verarbeitung
- Zugriff nur im erforderlichen Umfang (Least Privilege)
- Regelmäßige Überprüfung von Berechtigungen

e. Risikomanagement

- Kontinuierliche Bewertung der Risiken für die Rechte und Freiheiten betroffener Personen
- Anpassung der Schutzmaßnahmen entsprechend Risikolage, Stand der Technik und Verarbeitungskontext

f. Patch- und Schwachstellenmanagement

- Zeitnahe Installation von Sicherheitsupdates
- Strukturierter Patch-Management-Prozess
- Kontinuierliche Überwachung von Schwachstellen (z. B. über Sicherheitsquellen und Tools)
- Bewertung und Behandlung identifizierter Risiken

— Durchführung regelmäßiger Sicherheitstests (z. B. Penetrationstests)

5. Verschlüsselung und Schlüsselmanagement

— Verschlüsselung von Daten „at rest“ (z. B. AES-256 bei Datenbanken und Storage-Systemen)
— Verschlüsselung „in transit“ über TLS 1.2 / 1.3
— Zentrales Schlüsselmanagement (z. B. KMS)
— Zugriff auf kryptographische Schlüssel streng reglementiert

Stand: Juni 2026