

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOMS)

1. ZUTRITTSKONTROLLE

- Hosting der MiZeI-Anwendung in der AWS-Region Frankfurt (eu-central-1)
- Betrieb in zertifizierten Rechenzentren der Amazon Web Services (AWS) innerhalb der EU
- Physische Zutrittskontrollen durch den Rechenzentrumsbetreiber (mehrstufige Sicherheitskonzepte)

2. ZUGRIFFSKONTROLLE

- Rollen- und Rechtemanagement (Administrator / Nutzer)
 - Zugriff nur für berechtigte Personen
 - Starke Authentifizierungsmechanismen
 - Regelmäßige Überprüfung der Zugriffsrechte
 - Technische Durchsetzung
- „Krank“-Flag technisch getrennt von Zeitbuchungen

Für Sichtbarkeit von Krankmeldungen gilt:

- Mitarbeiter: nur eigene Krankmeldungen
- HR/Admin: vollständige Abwesenheitsübersicht

3. VERSCHLÜSSELUNG

- Verschlüsselte Datenübertragung (TLS)
- Verschlüsselung der Datenbankfelder mit Gesundheitsbezug
- Trennung zwischen Mandanten

4. EINGABEKONTROLLE

- Protokollierung von administrativen Zugriffen

5. TECHNISCHE DURCHSETZUNG DER ZUGRIFFSBESCHRÄNKUNGEN

- Rollenbasierte Zugriffskontrolle
- Technische Durchsetzung

6. AUFTRAGSKONTROLLE

- Weisungsgebundene Verarbeitung

7. VERFÜGBARKEITSKONTROLLE

- Regelmäßige, automatisierte Backups
- Redundante Systemarchitektur innerhalb der AWS-Region Frankfurt
- Maßnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit der Systeme

8. TRENNUNGSGEBOT

- Mandantentrennung je Kunde

9. DATENSCHUTZ DURCH TECHNIKGESTALTUNG

- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- Datensparsamkeit und Zweckbindung
- Mandantenbezogene Datenhaltung
- Dokumentierte Lösch- und Aufbewahrungskonzepte

10. DATENSPARSAMKEIT & EINGABEBESCHRÄNKUNG

- Kein Freitextfeld bei Krankmeldungen
- Keine Diagnosefelder oder medizinische Detaildaten
- Keine Upload-Pflicht für AU

11. ZWECKBINDUNG

Zulässige Zwecke:

- Abwesenheitsverwaltung
- Entgeltfortzahlung
- Personalplanung
- Erfüllung arbeitsrechtlicher Pflichten des Auftraggebers

Explizit ausgeschlossen sind:

- Leistungs- oder Verhaltensbewertung
- Gesundheitsprofile
- Statistische Auswertungen auf Personenebene

12. LÖSCHKONZEPT

- Technisch unterstützte Löschroutinen