

Anlage 5.4: Technisch-Organisatorische Maßnahmen (TOMs) des Auftragnehmers

(Zwingender Mindeststandard gemäß Art. 32 DSGVO und (ggf.) § 393 SGB V für die Verarbeitung von Patientendaten)

Der Auftragnehmer (AN) garantiert die Umsetzung und Aufrechterhaltung der folgenden Sicherheitsmaßnahmen für die gesamte Vertragslaufzeit. Soweit der AN für die Leistungserbringung fremde Rechenzentren oder Cloud-Infrastrukturen (Subunternehmer) nutzt, stellt der AN sicher, dass diese Subunternehmer die für sie relevanten Infrastruktur-Maßnahmen lückenlos und nachweisbar einhalten.

1. Zertifizierungen, Standards und Cloud-Sicherheit

- Informationssicherheits-Managementsystem (ISMS): Der AN unterhält ein aktives, zertifiziertes ISMS für seine Verarbeitungssysteme nach ISO/IEC 27001, BSI IT-Grundschutz oder einem gleichwertigen Framework (inkl. aktuellem Audit-Bericht).
- Cloud- & Rechenzentrums-Sicherheit (§ 393 SGB V): Wird für die Datenverarbeitung ein Cloud-Computing-Dienst oder ein externes Rechenzentrum eingesetzt, muss für die gesamte Infrastruktur ein gültiges BSI-C5-Typ2-Testat oder ein äquivalenter Nachweis gemäß den Bedingungen der C5-Gleichwertigkeitsverordnung (C5GleichwV) vorliegen und nachgewiesen werden.

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

- Zutrittskontrolle (Physischer Schutz der Rechenzentren und Geschäftsräume):
 - Unterbringung aller serverbasierten Systeme ausschließlich in nach ISO/IEC 27001 (oder gleichwertig) zertifizierten Rechenzentren o.Ä. mit Standort in Deutschland. Soweit der Bieter die serverbasierten Systeme in eigenen Räumlichkeiten (Inhouse) betreibt, befindet sich dieser spezifische IT-Betriebsbereich (Serverraum / Rechenzentrum) mitsamt den unterstützenden Infrastrukturen vollumfänglich in dem Geltungsbereich einer Zertifizierung nach ISO/IEC 27001 (oder gleichwertig), s.o.
 - Physische Absicherung der genutzten Gebäude und Geschäftsräume gegen unbefugten Zutritt während und außerhalb der Geschäftszeiten (z. B. durch einbruchshemmende Türen/Fenster, Schließanlagen oder eine Aufschaltung auf einen Sicherheitsdienst/Alarmanlage).
 - Elektronisches oder mechanisches Zutrittskontrollsystem (z. B. mittels codierter Chipkarten, Transponder oder einer dokumentierten Schlüsselordnung). Ein unbefugtes Betreten der Kernbereiche, in denen Patientendaten verarbeitet oder Server betrieben werden, ist technisch oder organisatorisch ausgeschlossen.
 - Besucherregelung: Zutritt für Dritte nur nach vorheriger Anmeldung und in ständiger Begleitung von autorisiertem Personal des AN bzw. des Rechenzentrumsbetreibers.
- Zugangskontrolle (Schutz vor unbefugter Systemnutzung):
 - Einsatz moderner Authentisierungsverfahren mit strengen Passwortrichtlinien (Länge, Komplexität).
 - Multi-Faktor-Authentisierung (MFA): Dies gilt zwingend für alle administrativen Zugänge (z. B. Administratoren, IT-Zertifizierte) sowie für jeden regulären

Mitarbeiterzugriff auf Systeme, über die produktive Patientendaten verarbeitet oder eingesehen werden können.

- Automatisches Sperren von Benutzersitzungen bei Inaktivität (Bildschirmsperre nach maximal 5 Minuten).
- Zentrale Verwaltung von Benutzerrechten durch ein Identity-Management-System; sofortige, automatisierte Sperrung von ausgeschiedenen Mitarbeitenden.
- Zugriffskontrolle (Schutz vor unbefugtem Lesen, Kopieren, Verändern):
 - Striktes Rollen- und Berechtigungskonzept nach dem „Need-to-know“-Prinzip (Mitarbeitende sehen nur Daten, die sie für ihre aktuelle Abrechnungsaufgabe zwingend benötigen).
 - Sichere Löschung und datenschutzkonforme Vernichtung von Datenträgern und Altpapier nach DIN 66399 (Schutzklasse 3). Für die Vernichtung von Papier gilt mindestens die Sicherheitsstufe P-5, für digitale Datenträger mindestens die Sicherheitsstufe E-4 oder gleichwertig.
 - Verbot der Nutzung von privaten Endgeräten (Bring Your Own Device / BYOD) für die Verarbeitung von Klinikdaten; ausschließliche Nutzung gehärteter Firmen-Laptops im Hinblick auf mobile Endgeräte
 - Zugriffe auf Systeme des Auftraggebers (Klinik) erfolgen ausschließlich personengebunden über Citrix oder definierte, vom Auftraggeber explizit freigegebene Schnittstellen
- Trennungskontrolle (Schutz vor Zweckentfremdung):
 - Strikte logische Mandantentrennung der Daten des Auftraggebers von den Daten anderer Kunden des AN in den Datenbanken
 - Voneinander physisch oder logisch getrennte Systemumgebungen für Entwicklung, Testlauf und den echten Produktivbetrieb. Eine Nutzung von echten Patientendaten in Testumgebungen ist strikt untersagt

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

- Weitergabekontrolle (Schutz bei Transport und Übertragung):
 - Verschlüsselung im Ruhezustand (Encryption at Rest): Sämtliche Datenbanken, Server-Festplatten und Backup-Medien, auf denen Patientendaten liegen, sind mit mindestens AES-256 (oder gleichwertig nach Stand der Technik) zu verschlüsseln.
 - Verschlüsselung bei der Übertragung (Encryption in Transit): Jeder Datenaustausch erfolgt über verschlüsselte Tunnel (VPN) oder mittels TLS 1.2 mit PFS (Perfect Forward Secrecy) oder höher (bevorzugt TLS 1.3)
 - Sperrung aller physischen Schnittstellen (USB-Ports, DVD-Laufwerke) an den Arbeitsplatzrechnern der Mitarbeitenden, um unbefugte Datenexporte zu verhindern
- Eingabekontrolle (Lückenlose Nachvollziehbarkeit):

- Revisionssichere Protokollierung aller Eingaben, Änderungen, Löschungen und Abrufe von Patientendaten.
- Die Protokolle müssen den Benutzer, die Uhrzeit, die Art der Aktion und den betroffenen Datensatz eindeutig identifizieren.
- Schutz der Protokolldateien vor nachträglicher Manipulation oder Löschung

4. Verfügbarkeit, Belastbarkeit und Notfallvorsorge (Art. 32 Abs. 1 lit. b & c DSGVO)

- Verfügbarkeitskontrolle (Schutz vor Datenverlust und Systemausfall):
 - Unterbrechungsfreie Stromversorgung (USV) und Notstromaggregate in den Rechenzentren
 - Einsatz von redundanten Systemkomponenten (RAID-Systeme, gespiegelte Serverarchitekturen)
 - Klimatisierung und automatisierte Brandmelde-/Löschsysteme in den Serverräumen
- Datensicherung, Archivierung & Ransomware-Schutz:
 - Tägliche Erstellung von Backups nach einem detaillierten Datensicherungskonzept.
 - Zwingende physische und/oder logische Trennung der Datensicherungen und Archivdaten vom Produktivnetzwerk, um eine Verschlüsselung der Backups durch Ransomware auszuschließen
 - Der AN garantiert die Einhaltung einer definierten maximalen Wiederherstellungszeit (RTO) im Notfall gemäß den Vorgaben des Hauptvertrags / Service Level Agreements (SLA)
- • Business Continuity (BC) & Disaster Recovery (DR):
 - Vorhalten detaillierter, dokumentierter Konzepte zur proaktiven Sicherstellung der Geschäftsfortführung (BCP) und zur reaktiven Notfallwiederherstellung (DRP)
 - Regelmäßige, dokumentierte Disaster-Recovery-Tests, um die Wiederherstellungszeiten zu überprüfen

5. Kontinuierliche Überwachung und Datenschutz-Management (Art. 32 Abs. 1 lit. d DSGVO)

- Cyber-Sicherheit & Incident Management (SIEM / SOC):
 - Betrieb eines kontinuierlichen Sicherheitsüberwachungssystems bestehend aus SIEM (Security Information and Event Management) und einem 24/7 SOC (Security Operations Center) zur Erkennung von unbefugten Zugriffen, Anomalien oder Ransomware-Angriffen o.Ä. in Echtzeit rund um die Uhr
 - Unverzögliche Einleitung automatisierter und/oder manueller Gegenmaßnahmen bei erkannten Anomalien
 - Einsatz von Endpoint-Detection-and-Response-Systemen (EDR) und tagesaktuellen Virenschannern
 - Durchführung von externen Penetrationstests auf den Abrechnungsplattformen (mindestens einmal jährlich)

- Meldung von Sicherheitsvorfällen:
 - Verpflichtung, den Auftraggeber über jeden Verdacht eines Sicherheitsvorfalls oder einer Datenpanne unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Bekanntwerden, detailliert zu informieren (Art. 33 Abs. 2 DSGVO); die Details der Meldewege werden im Auftragsverarbeitungsvertrag (AVV) konkretisiert.
- Auftragskontrolle & Berufsgeheimnis:
 - Regelmäßige Schulung und Sensibilisierung aller Mitarbeiter des AN zum Thema Datenschutz und IT-Sicherheit (mindestens einmal jährlich).
 - Verpflichtung nach § 203 StGB: Schriftliche Verpflichtung aller eigenen Mitarbeiter sowie der Mitarbeiter von Subunternehmern (sofern diese mit Patientendaten in Berührung kommen) auf die Wahrung von Amts- und Berufsgeheimnissen gemäß § 203 StGB vor Arbeitsaufnahme
 - Bestellung eines qualifizierten, betrieblichen Datenschutzbeauftragten