Technische und organisatorische Maßnahmen (TOM)

Version 1.1 – Aktualisiert am 07.01.2025

Optohive trifft geeignete technische und organisatorische Maßnahmen, um eine hohe Datensicherheit zu gewährleisten. Diese Maßnahmen berücksichtigen den Schutz von Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit personenbezogener Daten. Sie werden regelmäßig überprüft und entsprechend der neuesten technologischen Entwicklungen angepasst.

---

1. Vertraulichkeit

1.1 Zugriffskontrolle

Maßnahmen, um sicherzustellen, dass nur berechtigte Personen Zugriff auf personenbezogene Daten haben.

- **Technische Maßnahmen**:
    - Login mit Benutzername und Passwort.
    - Einsatz von Multi-Faktor-Authentifizierung (MFA) für sensible Systeme.
    - Verschlüsselung von mobilen Geräten und Datenträgern (z. B. Laptops, USB-Sticks).
    - Firewall und Zugriffsbeschränkungen für Cloud-Umgebungen.
    - Automatische Sitzungs-Timeouts in Software und Systemen.
- **Organisatorische Maßnahmen**:
    - Regelmäßige Schulungen der Mitarbeiter zu Datenschutz und Sicherheit.
    - Verwaltung von Benutzerrechten nach dem Prinzip der minimalen Berechtigung (Least Privilege).
    - Regelung zur Sperrung von Zugängen nach Ausscheiden von Mitarbeitenden.
    - Sicherstellung von Rollenkonzepten mit klaren Verantwortlichkeiten.

1.2 Zugangskontrolle

Maßnahmen, um unbefugten Zugang zu physischen und digitalen Infrastrukturen zu verhindern.

- **Technische Maßnahmen**:
    - Sicherheitsschlösser an sensiblen Türen.
    - Zugang zum Gebäude nur für autorisiertes Personal.
- **Organisatorische Maßnahmen**:
    - Zugang Gebäude mit Badge
    - Überprüfung von Besuchern in sensiblen Bereichen.
    - Begleitung externer Personen durch autorisiertes Personal.

- Keine papierbasierten Dokumente mit sensiblen Daten aufbewahren

---

2. Verfügbarkeit und Integrität

2.1 Datenträgerkontrolle

Maßnahmen, die sicherstellen, dass unbefugte Personen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten können.

- **Technische Maßnahmen**:
  - Verschlüsselung von physischen Datenträgern
  - Login mit Benutzername und Passwort
- **Organisatorische Maßnahmen**:
  - Kontrolle und Dokumentation des Einsatzes mobiler Speichermedien.
  - Sichere Entsorgung alter Datenträger durch zertifizierte Dienstleister.

2.2 Speicherkontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten sicher gespeichert werden und unbefugte Personen keinen Zugriff darauf haben.

- **Technische Maßnahmen**:
  - Login mit Benutzername und Passwort
  - Zugriffsbeschränkungen durch Benutzerrechteverwaltung und starke Authentifizierungsmechanismen.
  - Speicherung von Daten ausschließlich in verschlüsselten Datenbanken.
- **Organisatorische Maßnahmen**:
  - Festlegung von Richtlinien zur Zugriffsberechtigung auf Speichersysteme.
  - Regelmäßige Audits zur Überprüfung der Speichersicherheit.
  - Sicherstellung, dass nur autorisierte Personen Zugriff auf Speichersysteme haben.

2.3 Transportkontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten während der Übertragung vor unbefugtem Zugriff, Manipulation oder Verlust geschützt sind.

- **Technische Maßnahmen**:
  - Verschlüsselung der Datenübertragung über sichere Protokolle
  - Sicherstellung der Ende-zu-Ende-Verschlüsselung bei allen sensiblen Transfers.

    - Verwendung von sicheren Kommunikationskanälen, z. B. VPN für externe Zugriffe.

- **Organisatorische Maßnahmen**:
    - Sensibilisierung von Mitarbeitenden für den sicheren Umgang mit Daten während des Transports.

2.4 Wiederherstellung

Maßnahmen, die sicherstellen, dass Daten im Falle eines physischen oder technischen Zwischenfalls schnell wiederhergestellt werden können.

- **Technische Maßnahmen**:
    - Regelmäßige Erstellung von verschlüsselten Backups.
    - Verwendung eines sicheren externen Backupdienstleisters
    - Verwendung von redundanten Speicher- und Serversystemen.
    - Durchführung von Wiederherstellungstests, um die Funktionsfähigkeit der Backups zu überprüfen.
- **Organisatorische Maßnahmen**:
    - Aufbewahrung von Backups an einem sicheren, physisch getrennten Standort.
    - Dokumentierte Notfallpläne (Disaster Recovery) für verschiedene Zwischenfall-Szenarien.

2.5 Verfügbarkeit, Zuverlässigkeit und Datenintegrität

Maßnahmen, die sicherstellen, dass alle Systeme und Daten zuverlässig verfügbar sind, Fehlfunktionen erkannt werden und Daten vor unbeabsichtigter Veränderung geschützt sind.

- **Technische Maßnahmen**:
    - Einsatz von Spamfilter und regelmässige Aktualisierung
    - Server in sicheren Cloud-Rechenzentrum
    - Firewall bei Cloud-Providern
    - Monitoring-Tools zur Überwachung der Systemleistung und -sicherheit.
    - Regelmäßige Updates für Betriebssysteme und Anwendungen.
- **Organisatorische Maßnahmen**:
    - Regelmäßige Durchführung von Risikoanalysen, um Schwachstellen zu identifizieren.
    - Vertretungsregelungen für Mitarbeiter
    - Protokollierung und Dokumentation von Fehlermeldungen und Maßnahmen.

---

3. Nachvollziehbarkeit

3.1 Eingabekontrolle

Maßnahmen, um nachzuvollziehen, welche Personen welche Daten in Systemen eingegeben, geändert oder gelöscht haben.

- **Technische Maßnahmen**:
    - Individuelle Benutzerkennungen.
    - Protokollierung aller Eingaben und Änderungen (Logfiles).
- **Organisatorische Maßnahmen**:
    - Rechtevergabe für Eingabe, Änderung und Löschung nach festgelegten Berechtigungskonzepten.
    - Auswertung und Prüfung der Logfiles.

3.2 Bekanntgabekontrolle

Massnahmen, die gewährleisten, dass überprüft werden kann, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekannt gegeben werden.

- **Technische Maßnahmen**:
    - Login mit Benutzername und Passwort
    - Authentisierte und verschlüsselte Datenübertragung
    - Verwendung von auditierbaren Schnittstellen für Datenübermittlung.
- **Organisatorische Maßnahmen**:
    - Vertraulichkeitsvereinbarungen mit Drittanbietern und Subauftragnehmern.
    - Sorgfältige Auswahl von Unterauftragnehmern

3.3. Erkennung und Beseitigung

Massnahmen, die gewährleisten, dass Verletzungen der Datensicherheit rasch erkannt (Erkennung) und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können (Beseitigung).

- **Technische Maßnahmen**:
    - Regelmäßige Updates von Betriebssystemen und Anwendungen.
    - Schutz vor Malware durch aktuelle Virenscanner und Spamfilter.
    - Firewall bei Cloud-Providern
- **Organisatorische Maßnahmen**:
    - Dokumentierte Vorgehensweise bei Sicherheitsvorfällen.

- Regelmäßige Risikoanalysen zur Identifikation potenzieller Schwachstellen.

3.4. Export von personenbezogenen Daten

Optohive exportiert personenbezogene Daten nur in Länder, die ein angemessenes Datenschutzniveau gemäß DSG oder DSGVO gewährleisten.

3.5. Prüfung und Dokumentation

Optohive stellt sicher, dass die Einhaltung der technischen und organisatorischen Maßnahmen dokumentiert und regelmäßig geprüft wird.

Dieses Dokument ist Teil unserer Verpflichtung zur Einhaltung höchster Datenschutzstandards im medizinischen und wissenschaftlichen Umfeld.