Liste der technischen und organisatorischen Maßnahmen

Datenschutz-Management (technisch)

1. Datenschutz-Management-Tools - Software-Lösungen für Datenschutz , Management im Einsatz (Proliance 360)

Datenschutzfreundliche Voreinstellungen (technisch)

1. Datenminimierung - Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

Incident-Response-Management (technisch)

1. Spamfilter - Einsatz von Spamfilter und regelmäßige Aktualisierung

2. Virenscanner - Einsatz von Virenscanner und regelmäßige Aktualisierung

Weitergabekontrolle (technisch)

1. Webseitenverschlüsselung - Nutzung von Verschlüsselungstechnologie für die Website

2. Verschlüsselte Verbindungen - Bereitstellung über verschlüsselte Verbindungen wie sftp, https

Trennungskontrolle (technisch)

1. Berechtigungskonzept - Steuerung über Berechtigungskonzept

2. Mandanten-Trennung - Trennung der einzelnen Mandanten-Daten innerhalb der Anwendung

Verfügbarkeitskontrolle

1. Backupkonzept - Backup & Recovery-Konzept

- Einsatz redundanter Serverkomponenten zur Vermeidung von Single Points of Failure (SPoF)
- Automatisierte **Datenbank-Backups alle 6 Stunden** (maximaler potenzieller Datenverlust: 6 Stunden)
- **Tägliche vollständige Server-Backups**, physisch getrennt von der Produktionsumgebung gespeichert
- **Getestete Recovery-Strategie** mit Skripten zur Wiederherstellung aller Systeme
- **Wiederanlaufzeit (RTO):** vollständiger System- und Infrastruktur-Neuaufbau innerhalb von 60 Minuten

Monitoring & Protokollierung (technisch)

1. Lückenlose **Protokollierung aller Backend-Aktivitäten** (System- und Anwendungsebene)

2. Einsatz von **UptimeRobot** zur permanenten **Überwachung der Systemverfügbarkeit und Reaktionszeiten**

3. Nutzung der **DigitalOcean-Analytics** zur **Ressourcenüberwachung** (CPU, RAM, Netzwerk, Speicher) und **frühzeitigen Fehlererkennung**

Zugangskontrolle (organisatorisch)

1. Passwort-Richtlinien - regelmäßige Änderung, Mindestlänge, Komplexität etc.

2. Telefonate - Telefonate werden grundsätzlich hinter verschlossener Tür geführt

3. Videokonferenzen - Videokonferenzen werden grundsätzlich hinter verschlossener Tür mit

Sichtschutz geführt Zugangskontrolle (technisch)

1. Anti-Viren-Software Clients - Anti-Viren-Software Clients

2. Anti-Viren-Software Server - Anti-Viren-Software Server

3. Benutzerprofil Login - Login mit Benutzername + Passwort

4. Firewall - Einsatz einer Firewall

5. Passwortschutz - Zugang ist mittels eines Passworts geschützt

6. Datenträgerverschlüsselung - Verschlüsselung von Datenträgern in Laptops / Notebooks

Zugriffskontrolle/Pseudonymisierung (organisatorisch)

1. Autorisierter Zugriff - Zugriff nur für dafür autorisiertes Personal Zutrittskontrolle (organisatorisch)

1. Besucherbegleitung - Besucher in Begleitung durch Mitarbeiter

Regelmäßige Evaluierung

Die Wirksamkeit und Angemessenheit der technischen und organisatorischen Maßnahmen wird **mindestens einmal jährlich gemeinsam mit dem Datenschutzbeauftragten überprüft und dokumentiert**. Änderungen an Systemen oder Prozessen führen zu einer außerplanmäßigen Evaluierung. Die Ergebnisse und etwaige Anpassungen werden protokolliert.

Notfallpläne / Wiederherstellungsstrategie

Es besteht ein dokumentierter Notfall- und Wiederherstellungsplan.

Die Systeme werden alle 6 Stunden automatisch gesichert (maximaler potenzieller Datenverlust: 6 Stunden).

Zusätzlich erfolgen tägliche vollständige Server-Backups, die physisch getrennt von der Produktionsumgebung gespeichert werden.

Eine getestete Recovery-Strategie ermöglicht die Wiederherstellung aller Systeme innerhalb von 60 Minuten auf einer neuen Infrastruktur.

Die Wirksamkeit der Wiederherstellungsverfahren wird im Rahmen der jährlichen Evaluierung überprüft.

Schulungskonzepte

Alle relevanten Mitarbeiter werden regelmäßig durch einen externen Datenschutzdienstleister zu Datenschutz, Informationssicherheit und Meldepflichten geschult.

Teilnahmen und Schulungsinhalte werden dokumentiert.

Neue Mitarbeiter erhalten die Schulung unmittelbar nach Eintritt. Die Schulungskonzepte werden jährlich überprüft und bei Bedarf angepasst.