# Technisch organisatorische Maßnahmen TOM

**1. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**

- **Datenminimierung**: Unsere Anwendung ist so konzipiert, dass ausschließlich die Daten erhoben und verarbeitet werden, die für den jeweiligen Zweck erforderlich sind.
- **Zugriffskontrollen**: Es sind strenge Zugriffsmanagementrichtlinien implementiert, die durch AWS IAM-Richtlinien, Rollen und Berechtigungen den Zugriff auf personenbezogene Daten regeln.
- **Verschlüsselung**: Sämtliche personenbezogene Daten werden bei uns sowohl im Ruhezustand (z. B. durch AWS KMS und S3-Verschlüsselung) als auch während der Übertragung (z. B. via HTTPS und TLS) geschützt.
- **Sichere Voreinstellungen**: Unsere Infrastruktur setzt standardmäßig Sicherheitsfunktionen wie AWS Security Groups, Firewalls und VPC-Konfigurationen ein.

**2. Zugriffskontrolle**

- **Rollenbasierte Zugriffskontrolle (RBAC)**: Unsere Rollen- und Berechtigungsmodelle gewährleisten, dass der Zugriff auf personenbezogene Daten klar definiert und beschränkt ist.
- **Authentifizierung und Autorisierung**: Multi-Faktor-Authentifizierung (MFA) wird für alle Benutzerkonten und administrative Zugriffe verwendet. Ausgeloggt wird man nach 1 Woche Untätigkeit in der Anwendung. Wir nutzen magic links für den Login, somit ist keine Falschanmeldung möglich. Passwörter die durch credentials stuffing oder phishing gestohlen werden können, gibt es nicht.
- Starke Passwortrichtlinien sowie OAuth2/SAML-basierte Authentifizierung für Zugriffe auf die Infrastruktur sind integriert.
- **Zugriffsüberwachung**: Der Zugriff und Änderungen an sensiblen Ressourcen werden kontinuierlich durch AWS CloudTrail und andere Monitoring-Tools protokolliert.

**3. Physische Sicherheit**

- **AWS-Rechenzentrumssicherheit**: Unsere Lösung profitiert von den physisch gesicherten Rechenzentren von AWS, die kontrollierten Zugang, Überwachung und Redundanz bieten.
- **Verfügbarkeitszonen**: Durch den Einsatz von mehreren AWS-Regionen und Verfügbarkeitszonen stellen wir sicher, dass Daten jederzeit verfügbar sind und im Falle eines Ausfalls wiederhergestellt werden können.

**4. Datensicherheit**

- **Backups**: Wir setzen automatisierte, verschlüsselte Backups ein, die mit klar definierten Aufbewahrungsrichtlinien verwaltet werden.
- **Datenlöschung**: Für die dauerhafte und sichere Datenlöschung sind Mechanismen wie S3-Lebenszyklusrichtlinien etabliert.
- **Erkennung von Datenschutzverletzungen**: Zur Erkennung und Abwehr von Datenschutzverletzungen nutzen wir Systeme wie Amazon GuardDuty, AWS Config und AWS CloudWatch.

**5. Reaktion auf Vorfälle**

- **Protokollierung und Überwachung**:
  - AWS CloudWatch wird genutzt, um die Systemleistung und sicherheitsrelevante Ereignisse zu überwachen.
  - Änderungen an Ressourcen werden detailliert durch AWS CloudTrail aufgezeichnet.
  - Erweiterte Überwachungsfunktionen werden durch Drittanbieter-Sicherheitslösungen ergänzt.
- **Vorfallsmanagement**: Ein getesteter Plan zur Reaktion auf Sicherheitsvorfälle ist implementiert.
- **Benachrichtigungssystem**: Wir gewährleisten, dass im Falle eines Verstoßes sowohl Behörden als auch betroffene Personen innerhalb der vorgeschriebenen 72 Stunden benachrichtigt werden.

**6. Rechte der betroffenen Personen**

- **Recht auf Auskunft**: Wir stellen APIs und Benutzeroberflächen bereit, die es Nutzern ermöglichen, auf ihre personenbezogenen Daten zuzugreifen.
- **Recht auf Löschung**: Mechanismen zur Kontolöschung und Anonymisierung personenbezogener Daten sind vorhanden.
- **Recht auf Datenübertragbarkeit**: Die Bereitstellung personenbezogener Daten in einem standardisierten und maschinenlesbaren Format ist gewährleistet.

**7. Richtlinien für Mitarbeitende**

- **Zutritt zu den Unternehmensräumlichkeiten**: Unbefugten ist der Zutritt nicht möglich. GF verwaltet die Schlüssel. Mitarbeitende arbeiten remote ohne Zugang zu den Unternehmensräumlichkeiten.
- **Verschwiegenheitspflicht**: Alle Mitarbeitenden sind vertraglich zur Verschwiegenheit verpflichtet.
- **Umgang mit Betriebsgeräten**: Alle Betriebsgeräte werden den Mitarbeitenden von CERTAIN zur Verfügung gestellt. Die Nutzung von privaten Rechnern ist nicht gestattet.
- **Mitarbeiter-Umgang mit personenbezogenen Daten**: CERTAIN unterhält papierlose Büros. Personenbezogene Daten sind lt. 1., Absatz 2 Zugriffskontrollen geschützt. Fremdpersonal hat keinerlei Zugang zu Räumlichkeiten und Daten.
- **Schulungen Datenschutz:** Alle Mitarbeiter erhalten regelmäßig dokumentierte Unterweisungen durch den Datenschutzbeauftragen

CERTAIN GmbH, 5.12.2024