

Anhang B – Datensicherheitskonzept mit technischen und organisatorischen Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer der KSV GmbH mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

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

1. Maßnahmen der Zutrittskontrolle

- Sicherheitsschlösser
- Elektrische Türöffner
- Alarmanlagen
- Schlüsselregelung/Schlüsselbuch
- Klingelanlage mit Kamera
- Empfang mit Rezeption
- Begleitung der Besucher
- Alleinige Nutzung der Büros
- Abgegrenzte Serverräume (Sperrbereich)
- Einsatz von Wachpersonal
- Sorgfältige Auswahl von Dienstleistern

2. Maßnahmen der Zugangskontrolle

- (sichere) Kennwörter
- Anti-Viren-Software
- Firewalls (Software & Hardware)
- VPN-Technologie
- Vergabe von Nutzungsberechtigungen
- Identifikation und Authentifizierung der Benutzer
- Protokollierung der Benutzer und deren Aktivitäten
- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerrechten
- Nutzung von Active-Directory
- Allgemeine Richtlinie IT-Sicherheit/Datenschutz
- Passwortrichtlinie
- Einsatz eines Rechte- und Rollenkonzepts

3. Maßnahmen der Zugriffskontrolle

- Administrativer Zugang mit Änderungsberechtigung bei QiTEC
- Kunden-Zugang mit eingeschränkten Rechten
- Administrative Änderungen werden protokolliert
- Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
- Protokollierung von Zugriffen
- Begrenzung der Anzahl der Administratoren
- Sichere Aufbewahrung von Papierakten
- Verwaltung der benutzerrechte durch Administratoren
- Verwaltung der Benutzer durch Administratoren
- Abschließbare Schränke für Sicherungsdatenträger
- Datensicherungskonzept
- Physische Löschung von Datenträgern
- Differenzierte Berechtigungen (Anwendungen, Betriebssystem und Daten)
- Einsatz von Dienstleistern zur Aktenvernichtung
- Einsatz von Dienstleistern zur Datenträgervernichtung
- Home-Office-Richtlinie

4. Maßnahmen der Trennungskontrolle
 - Mandantenfähigkeit (Server getrennt von anderen Kunden: eigener IP-Bereich)
 - Instanzen (Docker-Container) sind jeweils getrennt
 - Physikalisch getrennte Speicherung
 - Getrennte Ordnerstrukturen
 - Gesonderte Systeme oder Datenträger
 - Berechtigungskonzepte
 - Datenbankrechte

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

1. Maßnahmen der Weitergabekontrolle
 - Ein unbefugter Zugriff ist nicht möglich (Zwei-Wege-Authentifizierung mit Key und IP)
 - Einsatz von Virtual Private Networks (VPN)
2. Maßnahmen der Eingabekontrolle
 - Einsatz eines Dokumentenmanagementsystems
 - Vergabe von rechten zur Eingabe, Änderung und Löschung von Daten
 - Nachvollziehbarkeit der Eingaben/Änderungen und Löschung durch individuelle Benutzernamen
 - Zuweisung von Zuständigkeiten für Eingabe, Änderung und Löschung von Daten

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

1. Maßnahmen der Verfügbarkeits- und Wiederherstellbarkeitskontrolle
 - Einsatz von Virenschutz-Software
 - Einsatz von Firewall (Hardware)
 - Einsatz von Firewall (Software)
 - Einsatz von RAID-Systemen
 - Implementierte Meldewege
 - Implementierte Notfallpläne
 - Backup-Strategie (online/offline; on-site/off-site)
 - Separate Sicherung der Backups
 - Tägliche Vollbackups der Instanzen
 - Wöchentliche Backups
 - Monatliche Backups
 - Unterbrechungsfreie Stromversorgung (USV)
 - Einsatz eines zertifizierten Rechenzentrums
 - Regelmäßige Tests zur Prüfung der Datenwiederherstellbarkeit
 - Regelmäßige Überprüfung der Rücksicherung
 - Trennung der Betriebssysteme und Daten (nach Partitionen oder Datenträgern)
 - Feuer- und Rauchmeldeanlage
 - Feuerlöscher vor dem Serverraum
 - Klimatisierter Serverraum
 - Überwachung der Server (Feuchtigkeit, Temperatur)
 - Überspannungsschutzeinrichtung
3. Maßnahmen der Belastbarkeitskontrolle
 - Einsatz von Hardware-Firewalls
 - Regelmäßige Sicherheitsupdates
 - Überwachung der Systeme hinsichtlich der Belastbarkeit

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs.1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

1. Maßnahmen des Datenschutzmanagements und Incident-Response-Managements
 - Bestellung eines (externen) Datenschutzbeauftragten
 - Erfassung der datenschutzrechtlichen Prozesse im QM-System
 - Implementation von Prozessen zum Umgang mit Betroffenenrechten
 - Regelmäßige Sensibilisierung / Schulung der Beschäftigten
 - Verpflichtung der Beschäftigten auf das Datengeheimnis
 - Vertretungsregelung
 - Implementation eines Notfallkonzeptes
 - Einbindung des Datenschutzbeauftragten bei Sicherheitsvorfällen
 - Sicherheitsvorfälle werden priorisiert persönlich vom Geschäftsführer bearbeitet und entsprechende Maßnahmen ergriffen
2. Maßnahmen der Auftragskontrolle
 - Eindeutige Vertragsgestaltung / Abschluss von Auftragsverarbeitungsverträgen
 - Sicherstellung der DSGVO-konformen Datenvernichtung bei Beendigung des Auftrags
 - Strenge Auswahl des Dienstleisters unter Sorgfaltsgesichtspunkten
 - Vorabprüfung der Sicherheitsmaßnahmen der Dienstleister
 - Verpflichtung von Dienstleister und deren Beschäftigten auf dessen/deren Vertraulichkeit und Geheimhaltung
3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
 - Es gibt keinen unautorisierten Zugriff auf die Systeme
 - Es werden nur zwingend notwendige Daten protokolliert