Technische und Organisatorische Maßnahmen (TOM)

Anlage 2 AV-Vertrag

Im Folgenden werden die technischen und organisatorischen Maßnahmen (TOM) zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung eines dem Risiko angemessenen Schutzniveaus insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen sowie der Belastbarkeit der Systeme.

Gemäß Artikel 32 DSGVO erfolgt dies unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

Die aufgeführten TOM gelten für die im Hauptvertrag definierten IT-Leistungen, welche in den unter Ziffer 1 angegebenen Rechenzentren erbracht werden.

1 Vertraulichkeit

Der Schutz personenbezogene Daten vor unbefugter Preisgabe.
(Artikel 32 Absatz 1 (b) DSGVO)

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Räumen zu verwehren, in denen sich Datenverarbeitungsanlagen befinden.

- Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den Zutritt zum jeweiligen Data Center nur für autorisierte Personen
- Autorisiertes Wachpersonal (Sicherheitsdienst vor Ort)
- Individuelle Zutrittsberechtigungsvergabe
- Zutrittskontrollsystem mit Chipkarten
- Büroräume außerhalb der Arbeitszeit sind verschlossen. Diese befinden sich jeweils im selben Gebäude. In beiden Rechenzentren ist an 365 Tagen im Jahr (inkl. Wochenende und Feiertage) Personal von mindestens 8:00 bis 23:00 Uhr vor Ort.
- Videokameras mit Daueraufzeichnung überwachen das Gebäude außen und innen
- Schutz der Infrastruktur durch Einbruchmeldeanlage (Alarmanlagengesichert)

- Schutz der Infrastruktur durch Rauchmelder / Brandmeldeanlage
- Schutz der Infrastruktur durch Rauchabzugsanlage
- Schutz der Infrastruktur durch Wassermelder

Die vorstehenden Punkte gelten für die Rechenzentren in München und Nürnberg und beruhen auf Angaben unseres Rechenzentrumsbetreibers und Dienstleisters für die technische Infrastruktur gemäß Anlage 1 AV für Subunternehmer / weitere Auftragsverarbeiter.

1.2 Zugangskontrolle

Es ist zu verhindern, dass Unbefugte Datenverarbeitungsanlagen nutzen können.

- Umsetzung einfacher Authentisierung per Username und Passwort
- Umsetzung sicherer Zugangsverfahren, starke Authentisierung
- Gesicherte (verschlüsselte) Übertragung von Authentisierungsgeheimnissen
- Monitoring kritischer Systeme
- Festlegung befugter Personen
- Sperrung bei Fehlversuchen / Logout bei Inaktivität
- Automatische Zugangssperre und manuelle Zugangssperre

1.3 Zugriffskontrolle

Es ist zu verhindern, dass auf Daten zugegriffen werden kann, für die keine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden.

- Erforderliche Mindestkomplexität für Kennwörter
- Erstellen eines Berechtigungskonzepts
- Vergabe minimaler benötigter Berechtigungen
- Verschlüsselte Speicherung von User-Passwörtern

1.4 Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt bearbeitet werden können.

- Datensparsamkeit im Umgang mit personenbezogenen Daten
- Trennung von Test- und Entwicklungsumgebungen

2 Integrität

Die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. (Artikel 32 Absatz 1 (b) DSGVO)

2.1 Eingabe- und Weitergabekontrolle

Ziel ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während Ihres Transports oder der Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Ebenso die Nachvollziehbarkeit von wem die Daten eingegeben, verändert, gespeichert oder entfernt wurden.

- Dokumentation der Vergabe von Zugriffsrechten inkl. Eingabeberechtigungen
- Administrative Aufgabentrennung
- Dokumentation der Weitergabe von physischen Speichermedien, mobile Datenträger
- Sichere Datenübertragung zwischen Server und Client
- Sicherung der Übertragung innerhalb der Systeme (Backend)
- Separate Instanzen für Entwicklungs- und Produktivsysteme
- Sichere Übertragung zu externen Systemen
- Datenschutzgerechtes Lösch- und Zerstörungsverfahren; Nutzung eines Aktenvernichters (mindestens Sicherheitsstufe 4 nach DIN 663994 = Besonders sensible Daten)

3 Verfügbarkeit und Belastbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können. Zur Sicherstellung der Belastbarkeit werden die nachfolgend genannten Maßnahmen unternommen. (Artikel 32 Absatz 1 (b) DSGVO)

- Schutz der Infrastruktur durch Hardware-Firewalls
- Software-Firewall
- Antivirus-Software auf allen Systemen
- Regelmäßige Software-Updates
- Tägliche inkrementelle Datensicherung
- Wöchentliche vollständige Datensicherung
- Wöchentliche Backups auf separat gespeicherten physischen Medien oder auf physikalisch getrennten Systemen
- Rauchmelder, Brandmeldeanlage, Rauchabzugsanlage Wassermelder
- Monitoring

4 Verarbeitung personenbezogener Daten nur nach Anweisung

Die Verarbeitung von personenbezogenen Daten ist nur entsprechend den Weisungen des Verantwortlichen zu verarbeiten (Auftragskontrolle).

- Abschluss einer Vereinbarung zur Auftragverarbeitung mit SpaceHost
- Abschluss einer Vereinbarung zur Auftragverarbeitung mit weiteren Auftragnehmern
- Schriftliche Verpflichtung aller Mitarbeiter auf die Wahrung der Vertraulichkeit
- Regelmäßige Datenschutz-Unterweisung der Mitarbeiter, Compliance-Regelung, Vertraulichkeitserinnerungen
- Datenschutzkonforme Löschung von Kopien und Sicherungen nach Abschluss des Auftrags

5 Verfahren zur regelmäßigen Überprüfung

Eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung hat stattzufinden. (Artikel 32 Absatz 1 (d) und Artikel 25 Absatz 1 DSGVO)

- Durchführung von technischen Überprüfungen
- Regelmäßige Überprüfung der Systemzugangsberechtigungen
- Regelmäßige Kontrolle externer Dienstleister