TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN nach Art. 32 DS-GVO

der

EURO VOIP GmbH
Bodenseestr. 217
81243 München

- im Folgenden Auftragsverarbeiter genannt -

Stand: 25.05.2021

Auftragsverarbeiter haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.

Die EURO VOIP GmbH erfüllt diesen Anspruch durch folgende Maßnahmen

1. Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Technische bzw. organisatorische Maßnahmen, nach dem jeweiligen Stand der Technik, zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- Manuelles Schließsystem
- Türen mit Knauf Außenseite
- Schlüsselregelung / Liste

2. Zugangskontrolle

Das Eindringen Unbefugter in die IT-Systeme ist zu verhindern.

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Login mit Benutzername + Passwort
- Anti-Virus-Software Clients
- Verwalten von Benutzerberechtigungen
- Richtlinie “Sicheres Passwort
- Anleitung “Manuelle Desktop-sperre"

3. Zugriffskontrolle

Unerlaubte Tätigkeiten in IT-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- Aktenschredder
- Protokollierung von Eingabe, Änderung und Löschung von Daten
- Differenzierte Berechtigungen
- Minimale Anzahl an Administratoren
- Verwaltung der Benutzerrechte durch Administratoren

4. Trennungskontrolle

Die getrennte Verarbeitung von Daten, die für unterschiedliche Zwecke gesammelt wurden.

- Trennung von Produktiv- und Testumgebung
- Mandantenfähigkeit relevanter Anwendungen
- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten

5. Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln (Elektronische Übertragung, Datentransport, Übermittlungskontrolle, usw.), um einen Verlust, eine Veränderung oder eine unbefugte Veröffentlichung zu verhindern.

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Bereitstellung über verschlüsselte Verbindungen wie sftp oder https
- Protokollierung (“Logging“).

6. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- Nachvollziehbarkeit von Eingäbe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

7. Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch / logisch):

- Backup- & Recovery-Konzept
- Sicherung der Daten in Cloud-Diensten

8. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten. Eine Datenverarbeitung durch Dritte (vgl. Art. 28 DSGVO) ist gemäß den Anweisungen des Auftraggebers/Datenexporteurs erlaubt.

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber/Datenexporteur und Auftragnehmer/Datenimporteur:

- Eindeutige Vertragsgestaltung
- Abschluss der notwendigen Auftragsverarbeitungsvereinbarung
- Schriftliche Weisungen an den Auftragnehmer
- Kontrolle der Vertragsausführung
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus