Technische- und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Managed Server | Managed VM

Dienstleistung: Managed Server / Managed VM

Anlage: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Die Vertragsparteien werden in ihrem jeweiligen Verfügungsbereich und bezogen auf den Vertragsgegenstand die technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO im erforderlichen sowie angemessenen Umfang und nach dem allgemein anerkannten Stand der Technik umzusetzen.
Die vom Auftragnehmer definierten und umgesetzten Maßnahmen sind teilweise abhängig vom Standort und können entsprechend variieren, ohne dass das erforderliche Sicherheitsniveau tangiert wird.
Im Einzelnen handelt es sich um folgende Maßnahmen:

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

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

Befindet sich der Server physikalisch im Bereich des Auftraggebers, so ist für die Zutrittskontrolle der Auftraggeber verantwortlich.
Befindet sich der Server in einem TelemaxX IPC, gelten die Festlegungen zur Zutrittskontrolle der Dienstleistung „Housing“ für die Managed Server / Managed VM entsprechend.

2. Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Für die Zugangskontrolle zur Anwendungsebene ist der Auftraggeber verantwortlich.
Im Verantwortungsbereich des Auftragnehmers befindet sich die Betriebssystemebene.
Ein Zugang und Zugriff auf die Anwendungsebene über die Betriebssystemebene kann für Administratoren technisch bedingt nicht ganz ausgeschlossen werden.

2.1 Betriebssystemebene

Maßnahmen	Beschreibung
Formales Vergabeverfahren für Zugangsberechtigung	Vergabe von Benutzerberechtigungen für TelemaxX-Mitarbeiter ist durch ein formales Verfahren festgeschrieben.
Zugang erst nach Anmeldung	Absicherung des Zugangs zur Betriebssystemebene durch Login-Prozess.
Zugangsberechtigung nach need-to-know-Prinzip	Nur die TelemaxX-Mitarbeiter erhalten Zugang zum Kundensystem (Betriebssystemebene), welche für dessen technische Betreuung zuständig sind.
Ausschließliche Verwendung von ausreichend sicheren Passwörtern	Richtlinien und Vorgaben für die Passwortsicherheit sind vorhanden.

2.2 Anwendungsebene

Maßnahmen	Beschreibung
Zugang nur nach Kundenweisung	Zugang auf Anwendungsebene ist TelemaxX-Mitarbeiter nur nach Weisung des Kunden erlaubt.
Verpflichtung aller TelemaxX Mitarbeiter auf Vertraulichkeit gem. Art. 28 Abs. 3 lit. b DSGVO und §3 TTDSG	TelemaxX-Mitarbeiter sind auf Datenschutz/ Vertraulichkeit, Fernmeldegeheimnis und zur Verschwiegenheit verpflichtet.
Datenschutzunterweisungen	TelemaxX-Mitarbeiter werden regelmäßig zu Themen des Datenschutzes unterwiesen.

3. Zugriffskontrolle

Es ist Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Für die Zugriffskontrolle zur Anwendungsebene ist der Auftraggeber verantwortlich.
Im Verantwortungsbereich des Auftragnehmers befindet sich die Betriebssystemebene.
Ein Zugang und Zugriff auf die Anwendungsebene über die Betriebssystemebene kann für Administratoren technisch bedingt nicht ganz ausgeschlossen werden.

3.1 Betriebssystemebene

Maßnahmen	**Beschreibung**
Formales Vergabeverfahren für Zugriffsberechtigung	Vergabe von Benutzerberechtigungen für TelemaxX-Mitarbeiter ist durch ein formales Verfahren festgeschrieben.
Berechtigungskonzept	Zugriffsrechte gemäß Berechtigungskonzept.
Begrenzung der Zugriffsmöglichkeiten	TelemaxX-Mitarbeiter erhalten nur Zugriff auf das System, wenn dies für die Aufgabenerfüllung notwendig ist.
Zugriffsberechtigung nach need-to-know-Prinzip	Nur die TelemaxX-Mitarbeiter erhalten Zugriff auf das Kundensystem (Betriebssystemebene), welche für dessen technische Betreuung zuständig sind.

3.2 Anwendungsebene

Maßnahmen	Beschreibung
Zugriff nur nach Kundenweisung	Zugriff auf Anwendungsebene ist TelemaxX-Mitarbeiter nur nach Weisung des Kunden erlaubt.
Verpflichtung aller TelemaxX Mitarbeiter auf Vertraulichkeit gem. Art. 28 Abs. 3 lit. b DSGVO und §3 TTDSG	TelemaxX-Mitarbeiter sind auf Datenschutz/ Vertraulichkeit, Fernmeldegeheimnis und zur Verschwiegenheit verpflichtet.
Datenschutzunterweisungen	TelemaxX-Mitarbeiter werden regelmäßig zu Themen des Datenschutzes unterwiesen.

4. Zwecktrennungsgebot

Es ist Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
Der Auftragnehmer hat keinen Zugang/Zugriff auf die Anwendungsebene (Software und/oder Datenbanken) des Auftraggebers. Für die Zwecktrennung bleibt der Auftraggeber verantwortlich.

Maßnahmen	**Beschreibung**
Mandantentrennung	Die Daten der TelemaxX-Kunden werden mit Hilfe geeigneter technischer Maßnahmen getrennt voneinander verarbeitet. Der Zugriff eines Kunden auf Daten eines anderen Kunden ist ausgeschlossen.

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

1. Weitergabekontrolle

Es ist Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

1.1 Managed Server

Maßnahmen	**Beschreibung**
Datenlöschung	Bei der Außerbetriebnahme der Hardware werden die Daten datenschutzgerecht gelöscht.
Datenträgerentsorgung	Die Entsorgung von Datenträgern erfolgt durch eine Fachfirma gemäß DIN 66399 (min. Klasse 2 / Stufe 4). Unterliegt ein defekter Datenträger der Gewährleistung wird eine einvernehmliche Lösung mit dem Kunden angestrebt.

1.2 Managed VM

Datenlöschung	Bei der Außerbetriebnahme der VM werden die Daten datenschutzgerecht gelöscht.

2. Eingabekontrolle

Es ist Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Für die Eingabekontrolle ist der Auftraggeber verantwortlich.

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

Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Die Verfügbarkeit der Daten und die Entscheidung über die Notwendigkeit einer Datensicherung liegt in der Verantwortung des Auftraggebers. Die Durchführung von Backups durch den Auftragnehmer kann entsprechend optional beauftragt werden.
Die Umsetzung sicherheitsrelevanter Updates (Patchmanagement) der Anwendungsebene liegt ebenso in der Verantwortung des Auftraggebers.
Befindet sich der Server in einem TelemaxX IPC, gelten die Festlegungen zur Verfügbarkeitskontrolle der Dienstleistung „TOM Housing“ für die Managed Server entsprechend.

Maßnahmen	**Beschreibung**
Backup (Betriebssystemebene)	Konfigurationsdaten auf Betriebssystemebene werden nach Beauftragung des Kunden gesichert.
Patchmanagement (Betriebssystemebene)	Sicherheitsrelevante Updates auf Betriebssystemebene können nach Beauftragung des Kunden durchgeführt werden.

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

1. Auftragskontrolle

Es ist eine auftrags- und weisungsgemäße Auftragsdatenverarbeitung zu gewährleisten.

Maßnahmen	**Beschreibung**
Handeln ausschließlich nach Kundenweisung	TelemaxX handelt ausschließlich im Rahmen und Umfang des Kundenauftrags entsprechend den dort festgelegten Weisungen.
Kontrollmaßnahmen	Kontrollmaßnahmen werden in Abstimmung zwischen Auftraggeber und Auftragnehmer definiert und technisch und organisatorisch in die Betriebsabläufe des Auftragnehmers eingebunden.
Verpflichtung aller TelemaxX Mitarbeiter auf Vertraulichkeit gem. Art. 28 Abs. 3 lit. b DSGVO und §3 TTDSG	Alle Mitarbeiter sind auf Datenschutz/ Vertraulichkeit, Fernmeldegeheimnis und zur Verschwiegenheit verpflichtet.
Datenschutzbeauftragter	Es ist ein Datenschutzbeauftragter bestellt. Email: datenschutz@telemaxx.de
Datenschutzunterweisungen	Mitarbeiter werden regelmäßig zu Themen des Datenschutzes unterwiesen.

2. Externe Prüfungen, Audits, Zertifizierungen

Der Auftragnehmer führt hinsichtlich der technischen und organisatorischen Maßnahmen regelmäßig folgende Prüfungen/Audits durch oder ist wie folgt zertifiziert:

Maßnahmen	**Beschreibung**
ISO 27001-Zertifizierung	Rechenzentren der TelemaxX sind nach ISO 27001 zertifiziert. Im Rahmen regelmäßig stattfindender Audits werden die Voraussetzungen für die Zertifizierung nachgewiesen.
Audits/Stichproben	In regelmäßigen Abständen werden vom Datenschutzbeauftragten und/oder IT-Sicherheitsbeauftragten Audits und/oder Stichproben durchgeführt.