



**Technische- und organisatorische Maßnahmen
gemäß Art. 32 DSGVO**

Managed Firewall | Router | Switch

Dienstleistung: Managed Firewall/Router/Switch

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 die Hardware physikalisch im Bereich des Auftraggebers, so ist für die Zutrittskontrolle der Auftraggeber verantwortlich.

Befindet sich die Hardware in einem TelemaxX IPC, gelten die Festlegungen zur Zutrittskontrolle der Dienstleistung „Serverhousing“ für die Managed Firewall/Router/Switch entsprechend.

2. Zugangskontrolle

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

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 durch Login-Prozess.
Zugangsberechtigung nach need-to-know-Prinzip	Nur die TelemaxX-Mitarbeiter erhalten Zugang zum Kundensystem, welche für dessen technische Betreuung zuständig sind.
Ausschließliche Verwendung von ausreichend sicheren Passwörtern	Richtlinien und Vorgaben für die Passwortsicherheit sind vorhanden.

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.

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, welche für dessen technische Betreuung zuständig sind.

4. Zwecktrennungsgebot

Es ist Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

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.

Maßnahmen	Beschreibung
Datenlöschung Datenträgerentsorgung	Bei der Außerbetriebnahme der Hardware werden die Daten datenschutzgerecht gelöscht. 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.

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.

Maßnahmen	Beschreibung
Protokollierung von Änderungen	Benutzeraktionen werden protokolliert.

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.

Befindet sich die Hardware in einem TelemaxX IPC greift ergänzend die Verfügbarkeitskontrolle „Serverhousing“. Befindet sich die Hardware in einem TelemaxX IPC, gelten die Festlegungen zur Verfügbarkeitskontrolle der Dienstleistung „Serverhousing“ für die Managed Firewall/Router/Switch entsprechend.

Verbindungsdaten werden nicht gesichert.

Maßnahmen	Beschreibung
Backup	Konfigurationsdaten werden bei Konfigurationsänderungen gesichert. Durch Beauftragung des Kunden kann zusätzlich eine Sicherung der Konfigurationsdaten durchgeführt werden.
Patchmanagement	Relevante Updates werden nach Vereinbarung mit dem Kunden durchgeführt.

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 TelemaxX-Mitarbeiter sind auf Datenschutz/ Vertraulichkeit, Fernmeldegeheimnis und zur Verschwiegenheit verpflichtet.
Datenschutzbeauftragter	Es ist ein Datenschutzbeauftragter bestellt. Email: datenschutz@telemaxx.de
Datenschutzunterweisungen	TelemaxX-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.