Technische- und organisatorische Maßnahmen gemäß Art. 32 DSGVO

TelemaxX Storage

Dienstleistung: Storage

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.

Die Storage-Systeme befinden sind in der Bundesrepublik Deutschland innerhalb TelemaxX eigener Rechenzentren.

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.

Maßnahmen	**Beschreibung**
Zutrittskontrollsystem	Elektronische Zutrittskontrolle bei Betreten des Rechenzentrums als auch in den jeweiligen Sicherheitsbereichen.
Absicherung der Zutrittskontrollsysteme	Zutrittskontrollsysteme sowie die Alarmanlagen sind über USV und Netzersatzanlage gegen Stromausfall gesichert. Im Falle einer Funktionsstörung kann der Zutritt zum Rechenzentrum über ein Sicherheitsschließsystem manuell erfolgen. Dies ist ausschließlich durch TelemaxX- Personal möglich.
Einrichtung von Sicherheitszonen	Der Zutritt zu den Storage-Systemen ist ausschließlich einem eingeschränkten Personenkreis (TelemaxX) möglich.
Schlüsselkonzept	Elektronisch: Der Zutritt ist durch ein materielles (RFID-Chip) und ein geistiges (PIN) Identifikationsmerkmal gesichert. Physikalisch: Die Racks des Storage-Systems verfügen über eine separate Schließung.
Zutrittserfassung	Jede Nutzung eines Coins (RFID-Chip) wird elektronisch

Maßnahmen	Beschreibung
	erfasst und mit Zeitdaten protokolliert.
Sicherheitspersonal	Das Rechenzentrum wird regelmäßig innerhalb vorgegebener Zeitfenster durch einen Wachdienst mithilfe von Video bestreift.
Einbruchmeldeanlage	Meldungen der Einbruchmeldeanlage (Einbruch, Störung etc.) werden auf unabhängigen Wegen an TelemaxX und den Wachdienst übertragen, welche entsprechend Maßnahmen einleiten.
Videoüberwachung	Die Außenhaut des Rechenzentrums und der Zutritt zu Sicherheitsbereichen im Rechenzentrum ist mit Videotechnik überwacht.
Closed-Shop-Betrieb	Das Gelände des Rechenzentrums dient nur dem Zweck der Datenverarbeitung, es besteht kein Publikumsverkehr.

2. Zugangskontrolle

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

Bei der Dienstleistung Storage ist zu unterscheiden zwischen der System-Managementebene und der Nutzdatenebene. Beide Ebenen sind voneinander strikt getrennt.

2. 1 Management:

Maßnahmen	Beschreibung
Ausschließlich personalisierter Zugang zum Storagesystem, nur ein Benutzerstammsatz pro Zugriffsberechtigtem	TelemaxX-Mitarbeiter haben nur personalisierten Zugang zum Storagesystem. Jeder Zugriffsberechtigte hat sein eigenes Benutzerkonto (keine Gruppenaccounts).
Ausschließliche Verwendung von ausreichend sicheren Passwörtern	Richtlinien und Vorgaben für die Passwortsicherheit sind vorhanden.

2. 2 Nutzdaten:

Maßnahmen	Beschreibung
Dedizierte physikalische Verbindung.	Direkte Kabelverbindung zwischen Kunde und Storagesystem
Zugangskennung für Speichervolumen	Eine Zugangskennung ist erforderlich und wird von TelemaxX an den Kunden kommuniziert.

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
Zugriff auf Nutzdaten ist nur für den Kunden möglich.	Ein Zugriff auf Nutzdaten seitens der TelemaxX oder des Wartungs-/Servicedienstleisters im Support/Wartungsfall ist systembedingt verriegelt.
Kunden haben nur Zugriff auf die eigenen Nutzdaten	Kundenspezifische Zugangskennungen erforderlich; diese werden von TelemaxX an jeweiligen Kunden kommuniziert. Einzelne Speichervolumen sind logisch getrennt.
Zentrale Vergabestelle für Zugangskennungen	Die Vergabe von Zugangskennungen für das Storagesystem erfolgt über eine zentrale Stelle.

4. Zwecktrennungsgebot

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

TelemaxX ist bei der Dienstleistung Storage im Rahmen der Zwecktrennung lediglich verpflichtet, die von den Kunden gebuchten Storage-Volumes getrennt zu speichern und zu verarbeiten. Für eine datenschutzkonforme Zwecktrennung innerhalb seiner Storage-Volume ist alleine der Kunde verantwortlich.

Maßnahmen	Beschreibung
Mandantentrennung	Die Daten der Kunden werden innerhalb der Storageplattform logisch getrennt vorgehalten und verarbeitet. Der Zugriff eines Kunden auf Daten eines

Maßnahmen	Beschreibung
	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
Dedizierte Leitungen zur Datenübertragung	Die Anbindung der Kunden an das Storagesystem ist im Einflussbereich der TelemaxX über dedizierte Leitungen und VLAN getrennt und entsprechend dokumentiert.
Datenträgerverwaltung	Es findet eine zentrale Datenträgerverwaltung statt. Die eingesetzten Datenträger sind dokumentiert.
Festmontierte Plattenspeicher	Die Datenverarbeitungs- und Speichersysteme sind im Rechenzentrum in den Racks fest eingebaut.
Kontrollierte und protokollierte Löschung einer Storage-Volume	Bei Vertragsende oder auf Verlangen des Kunden wird die komplette Storage-Volume gelöscht (Blockverweise auf die fragmentierten Daten werden gelöscht, anschließend werden die fragmentierten Daten automatisiert überschrieben).
Fernwartungskonzept (für Wartungs-/ Servicedienstleisters)	Zugang wird nur bei Bedarf und temporär freigegeben. Zugriff beschränkt auf Managementebene. Zugriff des Wartungs-/ Servicedienstleisters auf Nutzdaten ist nicht möglich.

5. 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.

Da von Seiten des Auftragnehmers ein Zugang und Zugriff auf Datenverarbeitungssysteme des Auftraggebers ausgeschlossen ist, können vom Auftragnehmer auch keine personenbezogenen Daten in das System des Auftraggebers eingegeben werden. Eine Eingabekontrolle obliegt dem Auftraggeber.

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 Systeme der Dienstleistung Storage sind in TelemaxX eigenen Rechenzentren untergebracht.
Die Sicherheit der Daten steht zusätzlich mit dem beauftragten Produktmerkmal (Gold, Silber oder Bronze) in Verbindung.
Die Verfügbarkeit der Daten und die Notwendigkeit einer Datensicherung liegt in der Verantwortung des Auftraggebers.

Maßnahmen	**Beschreibung**
USV (Unterbrechungsfreie Stromversorgung)	Das Rechenzentrum ist mittels USV-Anlage gegen kurzzeitige Stromausfälle abgesichert.
Notstromaggregate	Notstromaggregate sichern längere Stromunterbrechungen ab. Eine Nachbetankung während des Betriebes ist im Bedarfsfall möglich. Notstromaggregate werden nach Herstellervorgaben gewartet.
Brandschutz	Rechenzentrum ist in mehrere separate Brandabschnitte unterteilt. Zentrale Gaslöschanlage und zusätzliche Handfeuerlöscher zur punktuellen Brandbekämpfung.
Brandmelder	Brandmeldeanlage, welche die Gaslöschanlage auslöst und die Alarmierung der Feuerwehr, des Sicherheitsdienstes und des Bereitschaftshabenden der TelemaxX anstößt. Zusätzlich ist eine Brandfrühesterkennungsanlage installiert.
Klimatisierung	Das Rechenzentrum ist mit einer Raumklimatisierung ausgestattet.
Objektsicherung insb. der Storagesysteme	Die Storagesysteme sind innerhalb der Rechenzentren physikalisch durch verschlossene Schränke gesichert. Schlüsselkonzept, Videoüberwachung, Wachdienst usw.

Maßnahmen	Beschreibung
	sind gem. Beschreibung unter „Zutrittskontrolle“ vorhanden.
Option Storage Gold	Beim Produkt Storage Gold werden die Daten doppelt gespiegelt (4 fache Speicherung).Die Daten werden innerhalb eines physikalischen Systems gespiegelt (IPC3) Zusätzlich werden die Daten auf einem zweiten physikalischen System (IPC4) und dort ebenfalls innerhalb des Systems gespiegelt.
Option Storage Silber	Beim Produkt Storage Silber werden die Daten innerhalb eines physikalischen Systems (IPC) gespiegelt (doppelte Speicherung).
Option Storage Bronze	Beim Produkt Storage Bronze werden die Daten innerhalb eines RAID 5 Pools gespeichert.

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.