Technische- und organisatorische Maßnahmen gemäß Art. 32 DSGVO

TelemaxX Housing

Dienstleistung: Housing

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.

Maßnahmen	**Beschreibung**
Zutrittskontrollsystem	Elektronische Zutrittskontrolle bei Betreten des Rechenzentrums als auch in den jeweiligen Sicherheitsbereich.
Absicherung der Zutrittskontrollsysteme	Zutrittskontrollsysteme sowie die Alarmanlagen sind über USV und Netzersatzanlage gegen Stromausfall gesichert. lm Falle einer Funktionsstörung kann der Zutritt zum Rechenzentrum über ein Sicherheitsschließsystem manuell erfolgen. Dies ist ausschließlich durch TelemaxX-Mitarbeiter möglich.
Einrichtung von Sicherheitszonen	Der Zutritt zu den einzelnen Kundenschränken oder -flächen ist ausschließlich durch den Kunden und durch einen bei TelemaxX eingeschränkten Personenkreis möglich.
Schlüsselvergabe	An begrenzten Personenkreis, ausschließlich an autorisierte Personen (Whitelist), bei Übergabe

Maßnahmen	Beschreibung
	Identitätskontrolle mittels amtlicher Dokumente mit Lichtbild (z.B. Personalausweis), Dokumentation der Schlüsselübergabe.
Schlüsselkonzept	Elektronisch: Zutritt ist durch ein materielles (RFID- Chip) und ein geistiges (PlN) ldentifikationsmerkmal gesichert. Physikalisch: Jedes Kundenrack verfügt über eine eigene Schließung.
Besucherregelung	Besucher dürfen sich im Rechenzentrum ohne Begleitung von autorisiertem Personal oder TelemaxX-Mitarbeitern nicht aufhalten.
Zutrittserfassung	Jede Nutzung eines Coins (RFID-Chip) wird elektronisch erfasst und mit Zeitdaten protokolliert.
Sicherheitspersonal	Das Rechenzentrum wird regelmäßig innerhalb vorgegebener Zeitfenster durch eine Videobestreifung überwacht.
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.

Der Auftragnehmer hat keinen Zugang und Zugriff (im Sinne der Zugangskontrolle) auf die Datenverarbeitungssysteme des Auftraggebers (reines Housing). Für die Zugangskontrolle zu seinen Systemen ist der Auftraggeber verantwortlich.

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.

Der Auftragnehmer hat keinen Zugang und Zugriff (im Sinne der Zugriffskontrolle) auf die Datenverarbeitungssysteme des Auftraggebers (reines Housing). Für die Zugriffskontrolle zu seinen Systemen ist der Auftraggeber verantwortlich.

4. Zwecktrennungsgebot

Es ist Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
Da von Seiten des Auftragnehmers ein Zugang und Zugriff auf Datenverarbeitungssysteme des Auftraggebers ausgeschlossen ist, obliegt die Einhaltung des Trennungsgebots dem Auftraggeber.

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.

Der Auftragnehmer hat keinen Zugang und Zugriff (im Sinne der Zugangskontrolle) auf die Datenverarbeitungssysteme des Auftraggebers (reines Housing). Für die Weitergabekontrolle bezüglich seiner Daten ist der Auftraggeber verantwortlich.

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.

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.

Im Rahmen des Housing liegt die umgebungsbezogene Verfügbarkeit (Stromversorgung, Klimatisierung, Brandschutz) in der Zuständigkeit des Auftragnehmers.

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

Maßnahmen	Beschreibung
	Sicherheitsdienstes und des Bereitschaftshabenden der TelemaxX anstößt. Zusätzlich ist eine Brandfrühesterkennungsanlage installiert
Klimatisierung	Das Rechenzentrum ist mit einer Raumklimatisierung ausgestattet.
Objektsicherung insb. der Serverräume	Kundenschränke oder -flächen im Rechenzentrum sind physikalisch durch verschlossene Schränke bzw. Absperrungen der Flächen separat gesichert. Schlüsselkonzept, Videoüberwachung, Wachdienst usw. sind gem. Beschreibung unter „Zutrittskontrolle“ vorhanden.

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	TelemaxX Mitarbeiter sind auf Datenschutz/ Vertraulichkeit, Fernmeldegeheimnis und zur Verschwiegenheit verpflichtet.

Maßnahmen	Beschreibung
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	Die Dienstleistung „Housing“ ist in den Rechenzentren der TelemaxX nach ISO 27001 zertifiziert. (IPC 1, 3, 4 und 5) 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.