Technische- und organisatorische Maßnahmen gemäß Art. 32 DSGVO

TelemaxX Cloud

Inhaltsverzeichnis

1. Einleitung und Rahmenbedingungen

1.1 Einleitung

Unternehmen, die personenbezogene Daten erheben, verarbeiten, oder nutzen, haben technische und organisatorische Maßnahmen zu treffen, welche die Sicherheit und Integrität der Daten gewährleisten. Essentielle Teile dieser Maßnahmen möchten wir in diesem Dokument aufzeigen.

1.2 Unternehmen

TelemaxX Telekommunikation GmbH
Amalienbadstraße 41
76227 Karlsruhe
Deutschland

1.3 Externer Datenschutzbeauftragter

xDSB Datenschutz GmbH & Co. KG
Herr Rechtsanwalt Thomas Steinle LL.M.
Greschbachstraße 6a
76229 Karlsruhe
Deutschland

1.4 Geltungsbereich

Diese TOMs sind für die Cloud Services der TelemaxX gültig.

1.5 TelemaxX Cloud

Die Hardware der TelemaxX Cloud befindet sich redundant in mehreren hochsicheren Rechenzentren, deren Betreiber ebenfalls die TelemaxX ist. Der Rechenzentrumsbetrieb ist nach DIN EN ISO/IEC 27001 zertifiziert.

1.6 Datentransfer in Drittstaaten

Es werden keinerlei Daten aus der TelemaxX Cloud in Drittländer übertragen. Die Entsorgung von Datenträgern erfolgt gemäß DIN 66399 Schutzklasse 3. Im Gewährleistungsfall retournierte Festplatten enthalten Kundendaten ausschließlich in verschlüsselter Form.

2. Technische- und organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem folgendes ein:

2.1 Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen:

- Einsatz einer zwei-Faktor Authentifizierung für Zutritt zum Rechenzentrum
- Videoüberwachung
- Festlegung der zutrittsberechtigten Personen
- Closed Shop-Betrieb (nur berechtigte Personen haben Zutritt)
- Zutrittsregelungen für betriebsfremde Personen
- Revisionsfähigkeit der Zutrittsberechtigungen
- Schaffung von Sicherheitszonen
- Einsatz eines Zutrittskontrollsystems
- Schlüsselregelung und aktuelle Schlüsselliste
- Maßnahmen zur Innen- und Außenhautsicherung
- Protokollierung der Zutritte
- Sicherung durch Alarmanlage, und / oder Werkschutz

2.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahmen:

Kundenseite (Cloud Service Portal)

- Festlegung der nutzungsberechtigten Personen
- Identifikation und Authentifizierung der Benutzer
- Transportverschlüsselung der zu übertragenden Daten

Administration und Betrieb der Cloud durch TelemaxX

- Festlegung der nutzungsberechtigten Personen
- Identifikation und Authentifizierung der Benutzer
- Passwort-Länge entsprechend BSI-Guideline
- Sicherung der Datenstationen, Netze und Übertragungsleitungen
- Transportverschlüsselung der zu übertragenden Daten
- Separierte Management Infrastruktur
- Zentrales, firmenweites Identitätsmanagement
- 2FA-Authentifizierung per Firmen-Policy
- Zusätzliches Cloud-DevOPS Identitätsmanagement

2.1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, 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:

- Identifikation und Authentifizierung der Benutzer
- Maschinelle Überprüfung von Berechtigungen
- Einführung zugriffsbeschränkender Maßnahmen (Rollen und Entitlements)
- Transportverschlüsselung der zu übertragenden Daten
- Verschlüsselung der persistierten Daten (Encryption-at-Rest)
- Nutzer u. Zugriff auf das Cloud-Service-Portal durch den Kunden im Kundencenter definiert
- Optional 2FA einstellbar (durch den Kunden konfigurierbar)

Maßnahmen Cloud Infrastruktur & Management:
Generell:

- Zusätzliches zentrales Cloud-DevOPS Identitätsmanagement
- Passwort-Länge entsprechend BSI-Guideline

Aufbau der Managementnetze:

- Managementnetze sind von Kundennetzwerken per VLAN und per Firewall separiert
- Managementnetz: Outbound Internet-Access nur via Firewall, Inbound Internet-Access nicht möglich
- Management-Netzbereiche für die verschiedenen Anwendungsfälle (z.B. OOBM) sind nochmals per VLAN und Firewall abgetrennt

Netz- und Systemzugriff:

- VPN basierter Zugriff auf einzelne, dediziert freigegebene Hosts im Managementnetz. (VPN: TelemaxX-AD-Account mit 2FA)
- VPN-Zugriff auf JumpHost: Zugriff von JumpHost auf die Systemkomponenten mittels Cloud-DevOPS-Account
- VPN basierter Zugriff auf das gesamte Managementnetz (separater VPN User-Account)
- Login und Authentifizierung auf Systemkomponenten mittels Cloud-DevOPS-Account

Maßnahmen Arbeitsplatzsicherheit Mitarbeiterarbeitsplätze/ lokale Endpunkte:

- Lokale Datenträgerverschlüsselung per Firmen-Policy
- Lokale Virenscanner per Firmen-Policy
- Lokale Firewall per Firmen-Policy
- Lokales Endpoint Detection and Response (EDR)
- Hardening der OS-Einstellungen entsprechend BSI-Guideline
- Software-Updates per Firmen-Policy
- OS-Updates (Patchmanagement) per Firmen-Policy

2.1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Maßnahmen:

- Trennung von Test- und Produktivsystem
- Mandantentrennung - Logische Trennung von Daten und Netzwerken
- Durchführung und Dokumentation der Funktionstrennung

2.2 Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, 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:

- Für diesen Bereich nicht relevant, liegt im Einflussbereich des Kunden.

2.2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen:

- Für diesen Bereich nicht relevant, liegt im Einflussbereich des Kunden.

2.3 Pseudonymisierung und Verschlüsselung

2.3.1 Pseudonymisierung

Maßnahmen, die eine Pseudonymisierung von Daten gewährleisten.

Maßnahmen:

- Für diesen Bereich nicht relevant, liegt im Einflussbereich des Kunden.

2.3.2 Verschlüsselung

Maßnahmen, die eine Verschlüsselung von Daten gewährleisten.

Maßnahmen:

- Für diesen Bereich nicht relevant, liegt im Einflussbereich des Kunden.

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

2.4.1 Verfügbarkeit der Systeme

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Verfügbarkeit von Daten.

Maßnahmen:

- USV (Unterbrechungsfreie Stromversorgung)
- Notstromaggregat
- Brandschutz- und Katastrophenordnung
- Brandmelder
- Löschanlage (Gas)
- Klimatisierung
- Redundante Anbindungen (LWL und Energie)
- Wählbarer georedundanter Betriebsmodus (je nach Leistungspaket (SLC, Service Level Class))
- Dokumentiertes Konzept für Desaster Recovery

2.4.2 Belastbarkeit der Systeme

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Belastbarkeit der Systeme.

Maßnahmen:

- Update- bzw. Patchmanagement der Betriebsinfrastruktur
- Intrusion-Detection-and-Response-System
- Georedundanter Betrieb mit automatischer Umschaltung
- SIEM & XDR: Extended Detection and Response (XDR)
- Zentrale Analyse - Authentifizierungs-Logs, Firewall-Logs, VirenScanner-Logs

2.4.3 Wiederherstellbarkeit (der Daten / der Systeme)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Wiederherstellbarkeit von Daten und Systemen.

Maßnahmen:

- Schnelle Zugriffsmöglichkeit auf Ersatzteile bei technischen Ausfällen
- Redundante Serverstandorte vorhanden
- Einsatz von Virtualisierungstechnologie

2.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

2.5.1 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahmen:

- Abschluss der notwendigen Auftragsdatenvereinbarungen
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Schriftliche Anweisung an den Auftragnehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung eines Auftrags
- Überprüfung des Schutzniveaus des Auftragnehmers (initial)
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Überprüfung des Schutzniveaus des Auftragnehmers (kontinuierlich)
- Regelung zum Einsatz von Subunternehmern
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Geheimhaltung
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten (bei Bestellpflicht)
- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen

2.5.2 Datenschutz-Management

Maßnahmen, die gewährleisten, dass Methoden evaluiert wurden, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, organisieren, steuern und kontrollieren.

Maßnahmen:

- Bestellung eines externen Datenschutzbeauftragten
- Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz
- Durchführung von Datenschutzfolgeabschätzungen (bei Bedarf)
- Einhaltung der Informationspflichten gemäß Art. 13/ 14 DSGVO
- Evaluierung eines formalisierten Prozesses zur Bearbeitung von Auskunftsanfragen
- Regelmäßige Sensibilisierung der Mitarbeiter zum Datenschutz
- Schulung der Mitarbeiter zum Datenschutz
- Verpflichtung der Mitarbeiter auf das Datengeheimnis

2.5.3 Incident-Response-Management

Maßnahmen, die gewährleisten, das Sicherheitsvorfällen vorgebeugt werden kann oder im Falle von bereits eingetretenen Sicherheitsvorfällen, dass Daten und Systeme geschützt werden können und eine schnelle Analyse und Behebung des Sicherheitsvorfalls durchgeführt werden kann.

Maßnahmen:

- Dokumentation von Sicherheitsvorfällen
- Dokumentierter Prozess zur Meldung von Sicherheitsvorfällen
- Einbindung von Datenschutzbeauftragten in Sicherheitsvorfälle

- Einsatz eines Intrusion Detection Systems (IDS)
- Einsatz eines Intrusion Prevention Systems (IPS)
- Einsatz von Firewall und deren regelmäßige Aktualisierung

2.5.4 Datenschutzfreundliche Voreinstellungen

Maßnahmen, die gewährleisten, dass bereits durch die entsprechende Technikgestaltung (privacy by design) und Werkseinstellungen (privacy by default) eines Systems vorab ein gewisses Datenschutzniveau herrscht.

Maßnahmen:

- Auswahl der Systeme nach den Kriterien von privacy by design
- Auswahl der Systeme nach den Kriterien von privacy by default