TWL-KOM GmbH

Technische und Organisatorische Maßnahmen (TOM)
gemäß Art. 32 Absatz 1 Datenschutz-Grundverordnung (DS-GVO)

Version 1.3

Inhalt

Dokumenten-Historie

Version	Datum	Autor	Beschreibung
1.0	10.04.2018	TWL-KOM	Initiale Version
1.1	15.06.2019	TWL-KOM	Revision 1
1.2	02.04.2020	TWL-KOM	Ergänzungen Leistungsbeschreibung RZ II
1.3	03.09.2020	TWL-KOM	Ergänzung Zertifizierungen

Dokumenten-Klassifizierung

Status:	freigegeben
Freigabedatum:	03.09.2020
Dokumentenversion:	V1.3
Vertraulichkeitsklasse	Intern
Revisionszyklus:	12 Monate
Nächste Revision:	September 2021

1 Überblick

Dieses Dokument beschreibt die von TWL-KOM umgesetzten „technischen und organisatorischen Maßnahmen“ gemäß Art. 32 Absatz 1 DS-GVO. Die Maßnahmen gelten sowohl für TWL-KOM-eigene Systeme und Abläufe als auch für die für Kunden betriebenen Systeme und erbrachten Dienstleistungen. In dedizierten Vereinbarungen mit den jeweiligen Kunden können abweichende oder ergänzende technische und organisatorische Maßnahmen vereinbart sein.

2 Vertraulichkeit

2.1 Zutrittskontrolle

2.1.1 Zutrittskontrolle zu den Rechenzentren

Systeme von TWL-KOM und von TWL-KOM-Kunden sind in einem der von der TWL-KOM betriebenen Rechenzentren untergebracht.

2.1.1.1 Rechenzentrum I

Der Zugang zum Rechenzentrum I erfolgt mittels Codekarte und persönlicher Identifikation. Die TWL-KOM-Racks innerhalb der Rechenzentren sind abgeschlossen. Über Schlüssel verfügt nur die TWL-KOM. Dritte (z.B. Service-Techniker eines Herstellers) dürfen nur in Begleitung eines TWL-KOM Mitarbeiters im Rechenzentrum tätig werden. Der Zutritt zum Rechenzentrum wird protokolliert. Der Außenbereich, der Eingang und die RZ-Räume werden 24x7 videoüberwacht. Sowohl Türen als auch Räume werden über eine Alarmanlage überwacht. Bei einem Einbruchsversuch erfolgt automatisch eine Alarmierung. Scharf- und Unscharf Schaltung der Alarmanlage wird protokolliert.

2.1.1.2 Rechenzentrum II

Der Zugang zum Rechenzentrum II ist durch eine biometrische Personenvereinzelungsanlage geschützt. Die Authentisierung der zutrittsberechtigten Personen erfolgt mittels Codekarte und persönlicher Identifikation. Die TWL-KOM-Racks innerhalb der Rechenzentren sind abgeschlossen. Über Schlüssel verfügt nur die TWL-KOM. Dritte (z. B. Service-Techniker eines Herstellers) dürfen nur in Begleitung eines TWL-KOM-Mitarbeiters im Rechenzentrum tätig werden. Der Zutritt zum Rechenzentrum wird protokolliert. Der Außenbereich, der Eingang und die RZ-Räume werden 24x7 videoüberwacht. Sowohl Türen als auch Räume werden über eine Alarmanlage überwacht. Bei einem Einbruchsversuch erfolgt automatisch eine Alarmierung. Scharf- und Unscharf-Schaltung der Alarmanlage wird protokolliert.

2.1.2 Zutrittskontrolle zu den TWL-KOM Büroräumen

Der Zugang zu den TWL-KOM Büroräumen ist nur mittels Keycard und Schlüssel möglich. Der Zugang zu den Büroräumen der TWL-KOM wird 24x7 videoüberwacht. Besucher können die TWL-KOM-Räume ausschließlich über den Haupteingang und nur nach einer persönlichen Anmeldung am Empfang betreten.

2.2 Zugriffskontrolle

Zur Sicherstellung von Verfügbarkeit und Service-Qualität benötigen die TWL-KOM-Supportmitarbeiter je nach Dienstaufgaben in der Regel Vollzugriff auf die von TWL-KOM verantworteten und betriebenen IT-Systeme. Um unter diesen Umständen ein hohes Maß an Datenschutz zu gewährleisten, hat TWL-KOM die folgenden Maßnahmen implementiert:

1. Ein redundantes Firewall-System trennt die Arbeitsplätze, interne Server und Verwaltungssysteme der TWL-KOM vom Internet und von den Netzen der Kunden. Zu Netzen von Kunden besteht keine dauerhafte und direkte Verbindung. Diese wird lediglich im Bedarfsfall manuell und zeitlich beschränkt durch TWL-KOM Supportmitarbeiter hergestellt
2. Durch Konfiguration der TWL-KOM-Firewall, eventueller Kunden-Firewalls und der von TWL-KOM verwalteten Systeme wird sichergestellt, dass Zugriffe auf die von TWL-KOM verantworteten und betriebenen Systeme ausschließlich aus den Netzwerken des TWL-KOM Supports möglich sind.
3. Lediglich die Mitarbeiter des TWL-KOM Supports haben Zugang zu Kunden-Systemen. Innerhalb des Supports wird über Zugriffsrechte auf Basis der dienstlichen Notwendigkeiten weiter unterschieden.
   Der Zugriff des TWL-KOM Supports auf Zugangsinformationen (VPN-Einwahl, Systeminformationen und deren Zugangsdaten) von verwalteten Kundensystemen erfolgt über eine Applikation. Der Zugriff auf Zugangsinformationen von Kunden sowie der Login auf ein Kundensystem werden protokolliert.
4. Zugriffe auf verwaltete Systeme werden zusätzlich auf dem verwalteten System protokolliert.
5. Änderungen von Zugriffsrechten werden im Rahmen des Access-Managements geprüft, genehmigt und dokumentiert.
6. Alle Arbeitsplatzrechner bei TWL-KOM sind nach dem aktuellen Stand der Technik vor Schad-Software (Malware-Scanner), Datenverlust durch Diebstahl (Festplattenverschlüsselung) und unautorisiertem Zugriff geschützt.
7. Der Zugriff von TWL-KOM Arbeitsplätzen oder mobilen Systemen (z. B. Laptops) auf die von TWL-KOM verwalteten Produktivsysteme ist nur verschlüsselt (mittels HTTPS oder IPSec-VPN) möglich.
8. Der Zugriff von mobilen Systemen auf TWL-KOM-interne Systeme ist nur verschlüsselt (mittels HTTPS oder IPSec-VPN) und nach einer Mehr-Faktor-Authentifizierung möglich.
9. Ausscheidenden Mitarbeitern werden sämtliche Zutritts- und Zugriffsrechte mit dem Ausscheiden entzogen.

2.3 Trennungskontrolle

2.3.1 Dedizierte Systeme

Durch den Einsatz von dedizierten Server- und Storage-Systemen nutzen unterschiedliche TWL-KOM-Kunden jeweils ihre eigenen, exklusiven Ressourcen. Bei der Planung und dem Betrieb dieser „Exclusive Cloud Plattformen“ stellt TWL-KOM durch die folgenden Maßnahmen die korrekte Trennung der Kunden sicher:

1. Systeme von TWL-KOM und von TWL-KOM-Kunden sind auf Hardware-Ebene voneinander getrennt.
2. Eine gemeinsame Nutzung von Ressourcen durch verschiedene TWL-KOM Kunden besteht nicht.
3. Jeder Kunde verfügt über einen dedizierten Netzwerk-Bereich. Dieser ist durch Firewalls von anderen Kunden und von TWL-KOM getrennt.
4. Zur Verwaltung der Infrastruktur-Komponenten kommt ein abgeschottetes Management-Netz zum Einsatz, welches lediglich einen Zugriff auf die Hardwareebene ermöglicht (Betriebsparameter der Hardwareumgebung).

2.3.2 Shared Systeme

Durch den Einsatz von Server- und Storage-Virtualisierung nutzen unterschiedliche TWL-KOM-Kunden gemeinsame Ressourcen. Bei der Planung und dem Betrieb dieser „Shared Services“ stellt TWL-KOM durch die folgenden Maßnahmen die korrekte Trennung der Kunden sicher:

1. Systeme von TWL-KOM und von TWL-KOM-Kunden sind auf Hardware-Ebene voneinander getrennt.
2. Jeder Kunde verfügt über einen dedizierten Netzwerk-Bereich. Dieser ist durch Firewalls von anderen Kunden und von TWL-KOM getrennt.
3. Durch entsprechende Konfiguration der Server- und Storage-Virtualisierung werden die einzelnen Kunden voneinander abgeschottet.
4. Zur Verwaltung der Infrastruktur-Komponenten kommt ein abgeschottetes Management-Netz zum Einsatz, welches lediglich einen Zugriff auf die Hardwareebene ermöglicht (Betriebsparameter der Hardwareumgebung).

2.4 Pseudonymisierung

Bei der statistischen Auswertung von Zugriffen auf Web-Server von TWL-KOM und von TWL-KOM-Kunden wird die letzte Stelle der IP-Adresse gelöscht. So ist ein Rückschluss auf die zugreifende Person ausgeschlossen. Weitere Maßnahmen zur Pseudonymisierung personenbezogener Daten können kundenspezifisch implementiert werden.

3 Integrität

3.1 Weitergabekontrolle

Neben den Maßnahmen in Abschnitt „Zugriffskontrolle“ sind die folgenden Maßnahmen zum Schutz von Daten bei der Übertragung in Netzwerken bzw. bei der Speicherung auf Wechselmedien realisiert.

3.1.1 Datenaustausch

Der Austausch von elektronischen Daten firmenintern sowie zu Kunden, Partnern und Lieferanten erfolgt bei TWL-KOM fast ausschließlich über Netzwerke. Zum Schutz vertraulicher und insbesondere personenbezogener Daten setzt TWL-KOM hierbei auf Verschlüsselungstechniken:

- IPSec-VPNs zum Schutz der Kommunikation zwischen verschiedenen Netzen
- HTTPS-Kommunikation für Web-basierten Diensten
- TLS-verschlüsselte Kommunikation zwischen dem TWL-KOM-Mail-Gateway und den Mail-Gateways von Kunden, Partnern oder Lieferanten
- Verschlüsselter Dokumentenaustausch mit dem TWL-KOM-Produkt Datenaustausch Secure und Secure Customer Content

Die Übertragung unterliegt den vom Kunden dafür vorgegeben Schutzmaßnahmen.

3.1.2 Umgang mit Datenträgern und Festplatten

Daten von TWL-KOM und Kunden (und damit auch potenziell personenbezogene Daten) werden auf Festplatten gespeichert. Der Umgang mit Festplatten ist wie folgt geregelt:

1. Storage-Systeme, Server-Systeme mit lokalen Festplatten und Backupstorages werden ausschließlich in besonders zutrittsgesicherten Bereichen aufgebaut und betrieben.
2. Festplatten werden nach der Außer-Dienst-Stellung eines Speichersystems oder eines Servers von Mitarbeitern in den Räumen der TWL-KOM mit einer Löschstation gemäß BSI-Vorgaben überschrieben oder nach DIN66399 vernichtet.
3. Datenspeicher in Mobilgeräten (Festplatten in Laptops, Flash-Speicher in Mobiltelefonen oder Tablets) sind verschlüsselt und mit Passwort oder PIN gesichert. Soweit technisch möglich, werden Daten auf Mobilgeräten nach der Außer-Dienst-Stellung gelöscht.

3.2 Eingabekontrolle

Alle Änderungen an TWL-KOM-internen oder Kunden-IT-Systemen einschließlich der Eingabe, Modifikation oder Löschung personenbezogener Daten werden über das TWL-KOM-Ticket-System dokumentiert. Im Ticket sind hinterlegt:

- Welcher Kunde und welche(s) System(e) des Kunden sind betroffen?
- Welcher Mitarbeiter des Kunden hat den Auftrag erteilt (Meldeberechtigte)?
- Was sollte geändert, ergänzt oder gelöscht werden?
- Welcher TWL-KOM-Mitarbeiter hat den Auftrag ausgeführt?

Zusätzlich erfolgt eine Protokollierung von Aktionen über das zentrale Zugangsdaten-System der TWL-KOM und auf den einzelnen IT-Systemen. Art und Umfang der Protokollierung hängt dabei stark vom IT-System und den darauf laufenden Anwendungen, sowie den spezifischen Anforderungen des jeweiligen Kunden ab. Protokolle werden, wenn mit dem jeweiligen Kunden nicht anders vereinbart mindestens einen Monat aufbewahrt.

4 Verfügbarkeit und Belastbarkeit

4.1 Verfügbarkeitskontrolle

TWL-KOM ist spezialisiert auf das Hosting, die Implementierung und den Betrieb von hochverfügbaren IT-Lösungen. Dazu hat TWL-KOM an den beiden Rechenzentrums-Standorten in Ludwigshafen die folgenden Maßnahmen ergriffen:

1. Wo technisch sinnvoll möglich sowie kundenseitig gefordert, sind IT-Komponenten redundant ausgelegt. Zu diesen Redundanzmaßnahmen gehören zwei Netzteile, gespiegelte Festplatten, redundante Netzwerkanschlüsse, doppelte Controller.
2. Die Rechenzentren der TWL-KOM stellen folgende Leistungsmerkmale zur Verfügung:

   Rechenzentrum I
   - TWL-KOM Rechenzentrum, BSI-Grundschutz
   - Redundante 230V Stromversorgung mit Einspeisung über USV Anlagen (N+1)
   - Garantierte Stromverfügbarkeit: 99,99 % im Jahr
   - Die Rechenzentrumsflächen sind vollklimatisiert mittels redundanter Klimatechnik (N+1)
   - Garantierte Verfügbarkeit der Klimatechnik: 99,99 % im Jahr
   - Rauchansaugsystem zur Brandfrüherkennung
   - Zugangs- und Überwachungssystem
   - Zugang zur Rechenzentrumsfläche ist 24 Stunden am Tag an 365 Tagen im Jahr ohne Voranmeldung möglich, unter Berücksichtigung der Zugangsregelungen
   - Mehrfache Anbindung des Rechenzentrums an IP-Backbone-Netze mit hohen Bandbreiten

   Rechenzentrum II
   - TÜV geprüftes TIER 4 Rechenzentrum
   - IT-Grundschutz nach BSI, ISO/IEC 27001, ISO/IEC 27002, DIN EN 50600 und TIA-942, DSGVO
   - Redundante 230V Stromversorgung mit Einspeisung über USV Anlagen 2*(N+1)
   - Garantierte Stromverfügbarkeit: 99,99 % im Jahr
   - Die Rechenzentrumsflächen sind vollklimatisiert mittels redundanter Klimatechnik 2*(N+1)
   - Garantierte Verfügbarkeit der Klimatechnik: 99,99 % im Jahr
   - Rauchansaugsystem zur Brandfrüherkennung und Löschgasanlage
   - Zugangs- und Überwachungssystem, Biometrische Personenvereinzelungsanlage
   - Mehrfache Anbindung des Rechenzentrums an IP-Backbone-Netze mit hohen Bandbreiten

3. Umfang und Häufigkeit der Datensicherung werden zusammen mit dem Kunden auf Basis seiner Anforderungen festgelegt. Die Datensicherung wird durch TWL-KOM Mitarbeiter, entsprechend dem zwischen Kunde und TWL-KOM vereinbarten Sicherungsplan auf Vollständigkeit kontrolliert.

4.2 Belastbarkeit der Datenverarbeitung

TWL-KOM überwacht im Rahmen des Monitorings die Verfügbarkeit und wesentliche Betriebsparameter der IT-Systeme sowie der unterliegenden Virtualisierungslösung und Netzwerk-Komponenten. Damit werden akute Engpässe erkannt und es können Gegenmaßnahmen eingeleitet werden.
Darüber hinaus prüft TWL-KOM im Rahmen des regelmäßigen „Capacity-Managements“ die Entwicklung der Ressourcennutzung aller IT-Systeme. Bei sich abzeichnenden Engpässen informiert TWL-KOM den Kunden und stimmt gemeinsam nötige Erweiterungen ab. Je nach Kundenanforderungen implementiert TWL-KOM Mechanismen zur automatischen Lastverteilung und Angriffsprävention für einzelne Applikationen.

5 Regelmäßigen Überprüfung

5.1 Auftragskontrolle

Art und Umfang der IT-Dienstleistungen legen TWL-KOM und der Kunde im TWL-KOM-Systemschein fest. Dieses Dokument spezifiziert den Rahmen der IT-Dienstleistungen. Einzelne Teilaufträge im Rahmen der Support-Leistungen werden im TWL-KOM-Ticket-System als Change erfasst und dort für den Kunden sichtbar und nachvollziehbar dokumentiert.

5.2 Datenschutz-Management

Ein Datenschutzbeauftragter ist bestellt. Die Vorgaben der DS-GVO werden erfüllt, eine regelmäßige Überprüfung ist eingeführt.

5.3 Reaktion auf Datenschutzvorfälle

Bei Datenschutzvorfällen wird der Datenschutzbeauftragte der TWL-KOM unverzüglich hinzugezogen.

5.4 Datenschutzfreundliche Voreinstellungen

Soweit TWL-KOM Systeme (Plattform, Betriebssysteme, Datenbank, etc.) vorkonfiguriert zur Nutzung zur Verfügung stellt, sorgt TWL-KOM für datenschutzfreundliche Voreinstellungen (Privacy by Default).