Technisch-organisatorische Maßnahmen
M-net Telekommunikations GmbH

Technisch organisatorische Maßnahmen
gemäß Art. 32 DSGVO

ALLGEMEINES

Die M-net Telekommunikations GmbH stellt ihren Kunden Telekommunikationsleistungen zur Verfügung. Bei ihren Housing-Dienstleistungen sowie Connect-Leitungsverbindungen findet keine Verarbeitung oder Nutzung von personenbezogenen (Kunden-)Daten im Auftrag statt, welche nur bei Vorliegen solcher Verarbeitungsvorgänge eine sog. Auftragsverarbeitung i.S.d. Art. 28 DSGVO mit dem Kunden als Auftraggeber bedingen würde.

Die Housing-Dienstleistungen sind von einem „klassischen RZ“ zu unterscheiden: Bei den Housing-Dienstleistungen liegen im Gegensatz zu einer umfassenden RZ-Dienstleistung inkl. Server-Verwaltung und Hosting-Betreuung lediglich eine Bereitstellung der Flächen und Racks vor, ohne dass M-net Mitarbeiter in vertraglicher und sonstiger zulässiger Weise einen Zugriff auf die Kundenserver haben (dürfen), da diese vom Kunden selber in die RZ eingebracht und in eigener Verantwortung verwaltet und die Inhalte betreut werden. Die Verarbeitungsvorgänge von Kundendaten finden ausschließlich in den Servern statt, auf die M-net keinen Einfluss hat.

Im Übrigen erbringt M-net auch keine Wartungs- und Servicedienstleistungen an den Kunden-Servern, welche Anhaltspunkte für das Vorliegen einer ADV ergeben könnten.
Bei der Leistungserbringung für Sprach- und Datendienste findet hinsichtlich der Inhaltsdaten lediglich eine reine Durchleitung/Transport der analogen Signale bzw. der Datenpakete innerhalb der jeweiligen TK-Netzinfrastruktur statt. Die dabei anfallenden Verkehrsdaten werden wiederum nur im Rahmen der erforderlichen Leistungserbringung und nur innerhalb des gesetzlichen Maßstabes verarbeitet. Als TK-Netz- und Diensteanbieter unterliegt M-net bei der Erbringung ihrer TK-Dienste dabei mitunter den gesetzlichen Anforderungen und Bestimmungen des Telekommunikations- und ggf. Telemediengesetzes (TKG/TMG) und das Unternehmen hat das Fernmeldegeheimnisses zu beachten und zu wahren.
Aufgrund der in Bezug auf den Datenschutz und der Vertraulichkeit strengen gesetzlichen Bestimmungen des TKG/TMG und bereits aus Gründen des grundgesetzlichen Fernmeldegeheimnisses darf M-net, resp. ihre Mitarbeiter und Erfüllungsgehilfen de lege lata keine Einsicht über den Inhalt des Telefonie- und Datenverkehrs nehmen. Ein Verstoß gegen das Fernmeldegeheimnis ist bis hin zu einer Freiheitsstrafe auch strafbewehrt.

Technisch-organisatorische Maßnahmen
M-net Telekommunikations GmbH

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO): Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Vorh.	Prüfpunkt	Kommentar
Ja	1. Festlegung befugter Personen (Betriebsangehörige und Betriebsfremde)	Räume (v. a. Technikräume) sind verschlossen und können nur von berechtigten Personen betreten werden. Schlüsselverwaltung für mechanische und elektronische Schlüssel. Teilweise Zutrittsüberwachung
Ja	2. Regelung für Firmenfremde	Zutritt für berechtigte Betriebsfremde ist nach vorheriger Anmeldung (7x24) möglich. Schlüsselausgabe und Zutritt werden protokolliert. Betriebsfremde haben die „Richtlinie zum Arbeiten in Technikräumen von M-net“ zu beachten. Die Schränke der internen IT sind zusätzlich mit einem eigenen Schließkreis gesichert. Betriebsfremde haben hier keinen Zugriff. Zutritt in Sicherheitsbereiche durch firmenfremde erfolgt nur in Begleitung eines M-net Mitarbeiters
Ja	3. Anwesenheitsaufzeichnungen (Protokollierung)	Zutritt zu besonders schützenswerten Räumen wird überwacht, protokolliert und muss angemeldet werden
Ja	4. Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage und/oder Werkschutz	Sicherung teilweise durch Alarmanlage und Kameras. Es gibt keine ungeschützten Bereiche. Entweder via Alarmanlage, Werksschutz oder Videoaufzeichnung
Ja	5. Sicherheitsbereiche und wenige Zugangswege schaffen	Sicherheitsbereiche sind stets verschlossen, überwacht und nicht als solche erkennbar
Ja	6. Gegenseitige Überwachung (4-Augen-Prinzip)	Zutrittsüberwachung durch NOC
Ja	7. Entsprechende Ausgestaltung der Maßnahmen zur Objektsicherung (z. B. Spezialverglasung, Einbruchmeldesystem, Absicherung von Schächten, Geländebewachung)	Ist objekt- und verwendungsabhängig vorhanden

Technisch-organisatorische Maßnahmen
M-net Telekommunikations GmbH

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO): Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Ja	1. Verschließbarkeit von Datenstationen	Nutzung von Tresoren für Datenträger. Notebooks vom Vertrieb und GF sind größtenteils verschlüsselt. Alle personenbezogenen Daten sind im LAN, nicht auf der lokalen Festplatte gespeichert. Zusätzliche Sicherung der Notebooks mittels Kensington-Lock. Aktuell wird McAfee Safeboot für den unternehmensweiten Einsatz zur Verschlüsselung der Notebook-Festplatten evaluiert. Verschlüsselung von Emails nur auf Kundenwunsch
Ja	2. Identifizierung eines Terminals und/oder eines Terminalbenutzers gegenüber dem DV-System (z. B. durch Ausweisleser)	Authentifizierung über User/Passwort
Ja	3. Vergabe und Sicherung von Identifizierungsschlüsseln	Vergabe durch Bereichsleiter bzw. Geschäftsführer. Sicherung durch die Abteilung TE-IT-BE--
Ja	4. Regelung der Benutzerberechtigung	Vergabe durch Bereichsleiter bzw. Geschäftsführer. Sicherung durch die Abteilung TE-IT-BE--
Ja	5. Verpflichtung auf das Datengeheimnis	Wird bei jedem Mitarbeiter und extern Beschäftigten durchgeführt
Ja	6. Einsatz von Benutzercodes für Daten und Programme	Authentifizierung mittels single-sign-on oder Benutzernamen und Passwort
Nein	7. Einsatz von Verschlüsselungsroutinen für Dateien	Aktuell nicht im Einsatz
Ja	8. Differenzierte Zugriffsregelung (z. B. durch Segmentzugriffsperren)	Verschiedene Systeme sind getrennt gesichert. Des Weiteren gibt es für Systeme unterschiedliche Zugriffsrollen
Ja	9. Kontrollierte Vernichtung von Datenträgern	Vernichtung von Datenträgern über zertifiziertes Unternehmen

		(bei M-net Fa. Reißwolf). Dokumente und Datenträger werden mittels Datentonnen entsorgt. Festplatten, die nicht vernichtet werden, z.B. bei ausgemusterten Clients, werden ausgenullt. Firma Reißwolf ist nach DIN EN ISO 9001:2000 zertifiziert. M-net erhält Protokolle über die Vernichtung

3. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO): Zugriffskontrolle

Es ist zu 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.

Vorh.	Prüfpunkt	Kommentar
Ja	1. Datenstation mit Funktionsberechtigungsschlüssel	In den IT-Systemen sind Rollenstrukturen zur Differenzierung der Zugriffe implementiert
Ja	2. Regelung der Zugriffsberechtigung	Notwendige Zugriffe werden durch Bereichs- und Abteilungsleiter beantragt bzw. den technischen Systembetreuer Vergeben Neue Mitarbeiteraccounts werden mittels Workflow- Tool nach schriftlicher Genehmigung durch die entsprechenden Vorgesetzten (Bereichsleiter, Geschäftsführung) beantragt. Equipment (z.B. Laptop) wird nach Genehmigung durch Bereichs- bzw. Abteilungsleiter ausgegeben. Bei Abteilungswechsel werden die alten Rechte gelöscht und neue Rechte vergeben. IT prüft Berechtigungen

		regelmäßig auf Aktualität. Releases werden durch Fachabteilung freigegeben. IT-Security Dienstleister führt Security-Audit durch
Ja	3. Überprüfung der Berechtigung, maschinell z. B durch Identifizierungsschlüssel	Erfolgt im Rahmen eines Security-Audit
Ja	4. Auswertung von Protokollen Tägliche Auswertung von Server-Protokollen	Tägliche Auswertung von Server-Protokollen
Ja	5. Zeitliche Begrenzung der Zugriffsmöglichkeiten	Auto-Log-Off – Funktion bzw. Desktop-Sperre nach Zeit implementiert

4. Integrität (Art. 32 Abs. 1 lit. b DSGVO): Weitergabekontrolle

Es ist zu 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.

Vorh.	Prüfpunkt	Kommentar
Ja	1. Feststellung befugter Personen	Durch Vergabe von Rechten in Programmen (gemäß Punkt 2.3 / 2.)
Nein	2. Gegenseitige Überwachung (4-Augen-Prinzip)	Konzept ist in der IT erstellt
Nein	3. Ausgabe von Datenträgern nur an autorisierte Personen (z. B. Auftragsquittung, Begleitpapier)	Datenträger werden i. d. Regel nicht verwendet
Ja	4. Datenträger-Verwaltung Verwaltung	Verwaltung von Backup-Medien in IT und Technik. Datensicherung erfolgt zyklisch und unternehmensweit. Datensicherungen erfolgen unter der Woche inkrementell, am Wochenende werden Full-Backups erstellt.
Ja	5. Festmontierte Plattenspeicher	Systeme sind im Serverraum abgesperrt
Ja	6. Bestandskontrolle	Systeme sind alle produktiv, ein Fehlen / Ausfall des
Ja	7. Gesonderter Verschluss vertraulicher Datenträger	Tresor
Ja	8. Sicherheitsschränke	Tresor
Nein	9. Verbot der Mitnahme von Taschen und sonstigen Gepäckstücken in die Sicherheitsbereiche	Systeme sind teilweise gegen Nutzung von externen Speichermedien (z. B. USB-Sticks) gesichert
Ja	10. Kontrollierte Vernichtung von Datenträgern (z. B. Fehldrucke)	Ja, über Datenträgervernichtung (Fa. Reißwolf)

Technisch-organisatorische Maßnahmen
M-net Telekommunikations GmbH

Ja	11. Bestimmte autorisierte Benutzer	(gemäß Punkt 2.3 / 2.)
Offen	12. Verschlüsselung	--
Offen	13. Plausibilitätsprüfung	--
Offen	14. Vollständigkeits- und Richtigkeitsprüfung	--

5. Integrität (Art. 32 Abs. 1 lit. b DSGVO): Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.

Vorh.	Prüfpunkt	Kommentar
Ja	1. Nachweis der organisatorisch festgelegten Zuständigkeiten	Über Organisationsstruktur und Rechtevergabe
Ja	2. Protokollierung von Eingaben	Ja, Protokollierung mittels file-log. Löschen von Dateien wird protokolliert
Ja	3. Protokollierung der Dateibenutzung	Ja. Datensicherung mittels zyklischer Sicherung, pro Woche volle Sicherung auf Tapes, diese werden dann im Safe abgelegt. Datenbanksicherung mittels Recovery Manager und Datapump. Produktivdatenbanken sind als Data-Guard Umgebung über 2 Standorte verteilt. Überwachung der Datenbanken mittels Grid Control - Enterprise Manager
Ja	4. Verfahrens, Programm- und Arbeitsablauf-organisation	Prozesse und Arbeitsanweisungen
Ja	5. Verpflichtung auf das Datengeheimnis	Wird für alle Mitarbeiter durchgeführt

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO): Auftragskontrolle

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

Technisch-organisatorische Maßnahmen
M-net Telekommunikations GmbH

Vorh.	Prüfpunkt	Kommentar
Ja	1. Sorgfältige Auswahl der Auftragnehmer	Auswahl erfolgt über Fachbereiche direkt
Ja	2. Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber	Vertragliche Vereinbarung mit Auftragsdatenverarbeiter
Ja	3. Formalisierung der Auftragserteilung	Auftragnehmer und Auftraggeber
Ja	4. Kontrolle der Arbeitsergebnisse	Durch Fachabteilung
Ja	5. Kontrolle des Auftragnehmers bezüglich Einhaltung des Vertrages	Durch Fachabteilung und Datenschutzbeauftragten

7. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Es ist zu gewährleisten, dass Systeme und Dienste die Fähigkeit besitzen, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

Vorh.	Prüfpunkt	Kommentar
Ja	1. Backup-Verfahren, rasche Wiederherstellbarkeit (Art. 32 Abs. 1 c) DSGVO)	Erfolgt durch die Abteilung Abteilung TE-IT-BE-- im Wege von regelmäßig en Tages-/Wochen-/Monats-Backups
Ja	2. Katastrophen- oder Notfallplan (Wasser, Feuer, Explosion, Androhung von Anschlägen, Absturz, Erdbeben)	regelmäßige Abfrage der Fachbereiche von Risikoeinschätzungen durch den Fachbereich Qualitätsmanagement und Erstellung eines Riskoregisters und Maßnahmenkatalogs
Ja	3. Unterbrechungsfreie Stromversorgung (USV) Housing/ RZ	Zur Sicherung der unterbrechungsfreien Netzversorgung sind Systeme an einer statischen USV Anlage (n+1) angeschlossen

Technisch-organisatorische Maßnahmen
M-net Telekommunikations GmbH

8. Zweckbindungskontrolle (Art. 28 Abs. 3 S. 2 b) DSGVO)

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

Vorh.	Prüfpunkt	Kommentar
offen	1. Mandantentrennung	1. Mandantentrennung ---
Ja	2. Funktionstrennungen	Verschiedene Systeme zu unterschiedlichen Zwecken
Ja	3. Sicherstellung Trennung von Leitungen bei getrennter Wegeführung	Durch entsprechende Planung gewährleistet. Sofern eine Redundanz gefordert wird, wird diese auch wie angeboten realisiert. Hier sind die einzelnen Unterscheidungen zu beachten zwischen SNCP, MSP, getrennter Wegeführung, getrennter Hauszuführung. Maximale Verfügbarkeit 99,8% gemäß der „Leistungsbeschreibung M-net Connect“

9. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Ja	regelmäßige Überprüfung	kontinuierlicher Verbesserungsprozess wird durch Plan-Do-Check-Act Zyklus (PDCA-Zyklus) der mit dem nach ISO/IEC 27001 zertifizierten Informationssicherheits-Managementsystem ISMS umgesetzt