Vertrag über eine Auftragsverarbeitung nach Art. 28 DSGVO

(Anlage zum Vertrag für M-net V-Server)

zwischen

der _____

_____

_____

Vertragsnummer(n): _____
Kundennummer: _____

Auftraggeber (im Folgenden „AG“ genannt)

und

der **M-net Telekommunikations GmbH**
Emmy-Noether-Str. 2
80992 München

Auftragnehmer (im Folgenden „AN“ genannt)

alle gemeinsam im Folgenden „Parteien“ genannt.

1. Begriffsdefinitionen

1.1. **Personenbezogene Daten** sind Informationen im Sinne des Art. 4 Nr. 1 DSGVO.

1.2. **Verarbeitung** ist jeder Vorgang im Sinne des Art. 4 Nr. 2 DSGVO.

1.3. **Weisung** ist eine von AG erlassene und an den AN gerichtete Anordnung hinsichtlich der Verarbeitung von personenbezogenen Daten. Bestehende Weisungen (z. B. aus diesem Vertrag) können vom AG durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

2. Gegenstand und Dauer des Auftrags

2.1. Dieser Vertrag regelt den Rahmen der datenschutzrechtlichen Rechte und Pflichten bei der Verarbeitung personenbezogener Daten (im Folgenden „AG-Daten“) durch den AN für den AG in dessen Auftrag und nach dessen Weisungen im Sinne des Art. 28 DSGVO.

2.2. Der Gegenstand der Verarbeitung geht aus dem Hauptvertrag hervor, dem dieser Verarbeitungsvertrag angefügt ist.

2.3. Der Auftragnehmer nutzt die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

2.4. Der AG, oder der jeweilige AG des AG, ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er entscheidet über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten.

2.5. Der AN wird AG-Daten entsprechend den Weisungen des AG im Auftrag des AG unter Einhaltung der organisatorischen und technischen Vorgaben i. S. d. Ziff. 4. verarbeiten. Hierbei verpflichtet sich der AN besonders zu beachten:

- die technischen und organisatorischen Maßnahmen (Ziff. 4.)
- die Wahrung der Betroffenenrechte (Ziff. 5.)
- die besonderen datenschutzrechtlichen Pflichten (Ziff. 6.)
- die Vorgaben zu Unterauftragsverhältnissen (Ziff. 7.)
- die Kontrollrechte des AG und eines anderen Verantwortlichen (Ziff. 8.)
- die Mitteilungspflichten (Ziff. 9.)
- das allgemeine Weisungsrecht des AG (Ziff. 10.)
- die Rückgabe- und Löschpflichten (Ziff. 11.)

2.6. Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages (Ziff. 2.2.), sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

2.7. Die Parteien können diesen Vertrag jederzeit ohne Einhaltung von Kündigungsfristen aus wichtigem Grund kündigen. Ein wichtiger Grund liegt insbesondere vor,

- wenn ein schwerwiegender Verstoß des AN gegen gesetzliche Vorgaben oder gegen Pflichten aus diesem Vertrag vorliegt,
- wenn der AN eine Weisung des AG missachtet oder
- wenn der AN den Zugang des AG, des AG des AG, eines entsprechenden Beauftragten oder einer Datenschutzaufsichtsbehörde zu den Betriebsräumen, in denen AG-Daten aufgrund dieses Vertrages verarbeitet werden, vertrags- oder weisungswidrig verweigert.

2.8. Dieser Vertrag geht bei Widersprüchen bezüglich der Festlegung der datenschutzrechtlichen Pflichten, der Verantwortlichkeiten und der Konsequenzen allen anderen vertraglichen Regelungen vor, es sei denn, es wird mit ausdrücklichem Bezug auf diesen Vertrag etwas anderes vereinbart.

3. Umfang, Art und Zweck der vorgesehenen Verarbeitung, Datenarten und Kreis der Betroffenen

3.1. Art der Verarbeitung (Art. 4 Nr. 2 DSGVO) bei der Erbringung von folgenden Diensten:

M-net V-Server

3.2. Art der personenbezogenen Daten (Art. 4 Nr. 1, 13, 14 und 15 DSGVO):

☐ Personenstammdaten (Name, Vorname, Geschlecht, Geburtsdatum, Anschrift)

☐ Kommunikationsdaten (z. B. Telefon, E-Mail)

☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☐ Vertragsdaten/Bestelldaten

☐ Kundenhistorie

☐ Interessentendaten (Produktinteresse, Angaben zu Kaufabsichten, Angaben zu im Besitz befindlichen Produkten)

☐ Vertragsabrechnungs- und Zahlungsdaten

☐ Bank- oder Kreditkartendaten

☐ Befragungsergebnisse

☐ Personaldaten

☐ Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

3.3. Kategorien betroffener Personen (Art. 4 Nr. 1 DSGVO):

☐ Interessenten

☐ Kunden

☐ Beschäftigte und Stellenbewerber i. S. d. § 3 Abs. 11 BDSG

☐ Lieferanten/Dienstleister

☐ Handelsvertreter

☐ Sonstige: _____

4. Gewährleistung der technischen und organisatorischen Maßnahmen

4.1. Der AN bietet nach Maßgabe des Art. 28 Abs. 1 und 5 DSGVO hinreichende Garantien dafür, dass geeignete technische und organisatorische Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit der DSGVO und den Rechten der Betroffenen steht.

4.2. Der AN trifft geeignete technische und organisatorische Maßnahmen, die den Vorgaben des Art. 32 DSGVO entsprechen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, und unterstützt den AG bei der Einhaltung der in Art. 32 DSGVO genannten Pflichten. Der AN wirkt nach Maßgabe des Art. 28 Abs. 3 f) DSGVO bei der Erstellung einer Datenschutz-Folgenabschätzung i. S. d. Art. 35 DSGVO mit sowie bei der vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DSGVO. Er hat dem AG die erforderlichen Angaben und Dokumente auf Anfrage zur Verfügung zu stellen. Der AN erstellt ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO und übergibt dieses unaufgefordert dem AG.

4.3. Sofern die Auftragsvereinbarung vor Ort beim AG, beim Kunden oder per Fernwartung erfolgt, treffen die Pflichten aus dieser Ziffer 4 den AN nur, soweit die technischen und organisatorischen Maßnahmen in seinem Machtbereich liegen.

4.4. Die technischen und organisatorischen Maßnahmen unterliegen dem sich fortwährend entwickelnden Stand der Technik. Falls gesetzliche oder vertragliche Regelungen eine Anpassung bzw. Überarbeitung der in der Anlage 1 aufgeführten Maßnahmen des AN erforderlich machen, wird dieser die Maßnahmen auf eigene Kosten unverzüglich anpassen bzw. überarbeiten.

4.5. Kommt trotz entsprechendem Verlangen des AG keine Einigung über die Angemessenheit der technischen und organisatorischen Maßnahmen zustande, kann der AG alle zwischen den Parteien geschlossenen Verträge, die eine Verarbeitung von AG-Daten vorsehen, mit einer Frist von 14 Tagen zum Monatsende kündigen. Die verbleibenden Vertragsbestandteile können gleichermaßen gekündigt werden, wenn das Festhalten an ihnen aufgrund der Kündigung eine unzumutbare Härte für eine Vertragspartei darstellen würde.

5. Betroffenenrechte und Betroffenenklagen

5.1. Der AN erhält die Weisung, dem AG unverzüglich mitzuteilen, wenn ein Betroffener seine Rechte gemäß Art. 15–21 DSGVO i. V. m. §§ 34, 35, 36 BDSG geltend macht. Ebenso wird der AN den AG unverzüglich darüber informieren, wenn ihm eine Klage auf Grundlage des Art. 82 DSGVO zugeht.

5.2. Der AN wird ausschließlich nach Weisung des AG auf Betroffenenanfragen dieser Art reagieren.

5.3. Die Regelungen der Ziffern 5.1 und 5.2 gelten analog bei Anfragen und Prüfungen der Datenschutzaufsichtsbehörden, soweit AG-Daten mindestens mittelbar von solch einer Anfrage oder Prüfung berührt sind.

5.4. Der AN stellt sicher, dass Sperrungen von Daten sowie untersagte Verarbeitungen rechtskonform umgesetzt werden.

6. Besondere datenschutzrechtliche Pflichten des AN

6.1. **Datengeheimnis:** Den mit der Verarbeitung der AG-Daten beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit in geeigneter Weise und nachprüfbar auf das Datengeheimnis gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO zu verpflichten. Das Datengeheimnis muss auch nach Beendigung der Tätigkeit fortbestehen. Soweit andere Geheimhaltungsverpflichtungen (Fernmeldegeheimnis, Sozialgeheimnis etc.) zu wahren sind, wird der AN seine Beschäftigten entsprechend verpflichten.

Der AN hat bei der Auswahl und dem Einsatz der Beschäftigten sicherzustellen, dass diese die gesetzlichen Bestimmungen über den Datenschutz beachten und die aus der Sphäre des AG erlangten Informationen nicht an Dritte weitergeben oder zu einem anderen Zweck als dem Beauftragten verarbeiten (Art. 29 DSGVO).

Der AN wird auf Anforderung für den AG innerhalb von fünf Werktagen eine vollständige und jeweils aktuelle Liste der Beschäftigten, welche mit der Verarbeitung AG-Daten befasst sind bzw. vormals befasst waren, zur Einsicht bereithalten (Vorname, Name, einschl. eines verifizierbaren Nachweises über die Verpflichtung).

6.2. Der AN hat bei der Erstellung und Aktualisierung der Verarbeitungsübersicht des AG mitzuwirken. Dies umfasst nur Verarbeitungstätigkeiten, die im Rahmen der Auftragsverarbeitung für den AG vorgenommen werden.

6.3. Der AN unterstützt den AG gemäß Art. 28 Abs. 3 e) DSGVO mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seine Pflichten gegenüber den Betroffenen i. S. d. Kapitel 3 der DSGVO erfüllen kann.

6.4. **Beauftragter für den Datenschutz oder Vertreter:**

Der AN hat nach Maßgabe des § 38 BDSG i. V. m. Art. 37 DSGVO einen Beauftragten für den Datenschutz benannt und stellt sicher, dass dieser seine Tätigkeit gesetzeskonform ausüben kann. Dieser ist wie folgt zu erreichen:

M-net Telekommunikations GmbH

z. Hd. Datenschutzbeauftragter

Emmy-Noether-Str. 2

80992 München

datenschutz@m-net.de

Soweit der AN seinen Unternehmenssitz außerhalb der EU hat und somit keinen Datenschutzbeauftragten bestellen muss, benennt er einen Vertreter innerhalb der EU nach Maßgabe des Art. 27 DSGVO.

7. Begründung von Unterauftragsverhältnissen

7.1. Dem AN ist es gestattet, Unterauftragnehmer zur Erfüllung seiner vertraglichen Pflichten einzusetzen, sofern er den AG rechtzeitig (grundsätzlich 6 Wochen) vor der Datenverarbeitung hierüber informiert (Art. 28 Abs. 2 DSGVO). Zudem muss der AN dafür Sorge tragen, dass er den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat (Art. 28 Abs. 1 DSGVO).

7.2. Eine Einsetzung von in Drittländern ansässigen Unterauftragnehmern darf nur erfolgen, wenn zusätzlich die besonderen Voraussetzungen der Art. 44–50 DSGVO erfüllt sind.

7.3. Widerspricht der AG nicht innerhalb von 4 Wochen nach Erhalt der Information, akzeptiert er die Einsetzung als genehmigt im Sinne dieses Vertrages. Der AG kann der Einsetzung eines Unterauftragnehmers nur dann widersprechen, wenn dies ansonsten eine objektive Verschlechterung des bestehenden Datenschutzniveaus zur Folge hätte.

7.4. Der AN stellt sicher, dass der Unterauftragnehmer gegenüber dem AN in entsprechender Weise verpflichtet ist, wie der AN gegenüber dem AG nach dieser Vereinbarung verpflichtet ist. Der AN hat die Einhaltung dieser Pflichten des Unterauftragnehmers, insbesondere die Einhaltung der dort vereinbarten technischen und organisatorischen Maßnahmen, vor Beginn der Datenverarbeitung und sodann regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

7.5. Der AN stellt ferner sicher, dass der AG gegenüber dem Unterauftragnehmer die gleichen Kontrollrechte eingeräumt bekommt, wie der AG sie gegenüber dem AN selbst hat.

7.6. Der AN haftet gegenüber dem AG dafür, dass der Unterauftragnehmer den Datenschutzpflichten nachkommt, die ihm durch den AN im Einklang mit 7.1, 7.4 sowie 7.5 vertraglich auferlegt wurden.

7.7. Zurzeit verarbeiten die in Anlage 1 genannten Unterauftragnehmer personenbezogene Daten im Auftrag des AN. Der AG gestattet den Einsatz dieses Unterauftragnehmers, soweit jeweils die Pflichten aus 7.1, 7.4 sowie 7.5 erfüllt wurden.

8. Kontrollrechte des AG, Mitwirkungs- und Duldungspflichten des AN

8.1. Der AG, der Auftraggeber des AG oder dessen schriftlich Beauftragter haben das Recht, die Befolgung sämtlicher Weisungen und Bestimmungen dieser Vereinbarung durch den AN zu verlangen und nach schriftlicher Vorankündigung von vierzehn (14) Werktagen (mit sachlichem Grund – insbesondere nach Beschwerdefällen auch ohne schriftliche Ankündigung) zu den üblichen Geschäftszeiten zeitlich und räumlich unbeschränkt auf dem Grundstück und in den Geschäftsräumen des AN zu kontrollieren.

8.2. Dies umfasst insbesondere die Überprüfung der technischen und organisatorischen Maßnahmen vor Beginn der Datenverarbeitung und weitere regelmäßige Überprüfungen, insbesondere der geforderten Datenschutz- und Sicherheitsmaßnahmen.

8.3. Der AN verpflichtet sich, entsprechende Überprüfungen zu dulden, Zugang, Auskunft und Einsicht in alle dazu erforderlichen Unterlagen und Datenverarbeitungssysteme zu gewähren.

8.4. Über die Kontrolle und deren Ergebnisse ist ein Protokoll anzufertigen, das vom AG, vom Auftraggeber des AG und AN bzw. von deren Beauftragten zu unterzeichnen ist.

9. Mitteilungspflichten des AN

9.1. Der AN wird den AG unverzüglich von jedem Empfang von Anfragen oder Aufforderungen von einem Betroffenen oder einer Datenschutzaufsichtsbehörde bezüglich des Gegenstandes dieses Vertrages, insbesondere nach Ziff. 5.1., informieren.

9.2. Dem AN ist bekannt, dass der AG verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und gegebenenfalls der Datenschutzaufsichtsbehörde bzw. den Betroffenen binnen 72 Stunden zu melden (Art. 33 DSGVO). Sofern es zu solchen Verletzungen gekommen ist, wird der AN den AG bei der Einhaltung seiner Meldepflichten unterstützen. Er wird die Verletzungen dem AG melden und hierbei zumindest folgende Informationen bereitstellen:

- eine Beschreibung der Art der Verletzung, der betroffenen Datenkategorien sowie die ungefähre Zahl der Betroffenen und Datensätze.
- Name und Kontaktdaten eines Ansprechpartners für weitere Informationen.
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung.
- eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

9.3. Mitteilungen nach Ziff. 9.1. und 9.2. müssen unverzüglich, jedoch nicht später als innerhalb von 24 Stunden in Textform (z. B. Brief, Telefax oder E-Mail) übermittelt werden.

10. Weisungsrecht des AG, Haftungsfreistellung

10.1. Der AN verarbeitet AG-Daten ausschließlich im Rahmen dieser vertraglichen Vereinbarung und weiterer Weisungen des AG.

10.2. Der AG wird weitere Weisungen (fern)mündlich, per Brief, Fax oder E-Mail erteilen. (Fern)mündlich erteilte Weisungen sind vom AN zu dokumentieren.

10.3. Weisungsberechtigt sind die Geschäftsführer des AG sowie die jeweiligen Kontaktpersonen des AN beim AG.

10.4. Ist der AN der Ansicht, dass eine Weisung gegen die DSGVO oder sonstige Datenschutzvorschriften der Europäischen Union bzw. der Bundesrepublik Deutschland verstößt, weist der AN den AG unverzüglich per Brief, Telefax oder E-Mail darauf hin. Der AN ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie vom AG ausdrücklich bestätigt wird.

10.5. Der AN ist gegenüber dem AG verantwortlich für die Einhaltung seiner Verpflichtungen aus diesem Vertrag. Sofern Verstöße des AN gegen die Bestimmungen dieses Vertrags oder Einzelweisungen des AG zu Rechtsverletzungen führen, stellt der AN den AG von Ansprüchen Dritter frei; außerdem übernimmt der AN die erforderlichen Kosten der Rechtsverteidigung.

10.6. Der AN darf Verarbeitungen von AG-Daten nur dann ohne Weisung des AG durchführen, wenn er aufgrund einer Vorschrift der DSGVO oder einer sonstigen Rechtsvorschrift der Europäischen Union bzw. eines Mitgliedsstaates der Europäischen Union, der der AN unterliegt, hierzu verpflichtet ist. Der AN informiert den AG hierüber, bevor er mit der Verarbeitung beginnt, soweit ihm eine solche Mitteilung nicht durch eine anwendbare Rechtsvorschrift untersagt ist.

11. Rückgabe- und Löschungspflichten

11.1. Sofern keine gegenteilige Weisung erteilt wird, hat der AN dem AG bei Beendigung des Auftrags die ihm überlassenen Datenträger und Dokumente herauszugeben.

11.2. Weiterhin sind bei Beendigung des Auftrags vom AN verwendete AG-Daten – wenn nicht bereits zuvor geschehen – zu löschen, zu vernichten oder dem AG zu übergeben.

11.3. Auf Anfrage des AG bestätigt der AN, dass der AN die überlassenen Daten vollständig zurückgegeben, vernichtet bzw. unwiederbringlich gelöscht hat.

11.4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind vom AN für mindestens drei Jahre nach Ende ihrer Geltungsdauer aufzubewahren. Der AN kann bei Vertragsende die Dokumentationen zu seiner Entlastung dem AG übergeben.

11.5. Die Pflicht zur Löschung bzw. Vernichtung besteht nicht, solange eine gesetzliche Aufbewahrungspflicht entgegensteht.

12. Haftung und Schadensersatz

AG und AN haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

13. Schlussbestimmungen

13.1. Sollte Eigentum des AG beim AN durch Maßnahmen Dritter (z. B. Pfändung, Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet sein, so hat der AN den AG unverzüglich hierüber in Kenntnis zu setzen. Ein Zurückbehaltungsrecht in Bezug auf Datenträger oder Datenbestände des AG ist ausgeschlossen. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlicher im Sinne der Datenschutz-Grundverordnung liegen.

13.2. Die Einrede des Zurückbehaltungsrechts i. S. d. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der dazugehörigen Datenträger ausgeschlossen.

13.3. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Die Änderung bzw. Ergänzung kann auch in einem elektronischen Format (Textform) erfolgen (Art. 28 Abs. 9 DSGVO).

13.4. Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrages zum Datenschutz den Regelungen des Hauptvertrages (Ziff. 2.2.) vor. Sollte eine der vorliegenden Regelungen unwirksam sein, so berührt dies nicht die Wirksamkeit der übrigen Bestimmungen.

13.5. Die Anlage 2 (Technische und organisatorische Maßnahmen) ist Bestandteil dieses Vertrags.

13.6. Es gilt deutsches Recht.

Gezeichnet M-net Telekommunikations GmbH, Geschäftsführung im Juni 2018

…….…….. …….……..
Ort, Datum Unterschrift Kunde

ANLAGE 1: Unterauftragnehmer

1.

Derzeit keine Unterauftragsverhältnisse

ANLAGE 2: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

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

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	Datenträger werden i. d. Regel nicht verwendet

	Personen (z. B. Auftragsquittung, Begleitpapier)	
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)
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.

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

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