Vertrag zur Auftragsverarbeitung nach Artikel 28 DSGVO

zwischen dem/der

.....

– Verantwortlicher –

(im Folgenden: **Auftraggeber**)

und der

HEAG mobilo GmbH, Klappacher Str. 172, 64285 Darmstadt

– Auftragsverarbeiter –

(im Folgenden: **Auftragnehmer**)

(gemeinsam im Folgenden: **Vertragspartner)**

1. Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags ergibt sich aus

☐ der Vereinbarung der Vertragspartner über die Bereitstellung und den Betrieb eines Verkehrsmanagementsystems (VMS) sowie die Erbringung von Dienstleistungen einer Verkehrsleitstelle (VLS) vom….. (Datum einfügen)

und/oder

☐ der Vereinbarung der Vertragspartner über die Überlassung eines ÖPNV-Fahrkartenvertriebssystems und der Verarbeitung von Vertriebsdaten vom….. (Datum einfügen)

und/oder

☐ dem Mietvertrag über VMS- und Vertriebssystemkomponenten vom….. (Datum einfügen)

(im Folgenden: **Leistungsvereinbarung**).

(2) Die Leistungsvereinbarung betrifft

☐ folgende(s) Linienbündel ……..

und/oder

☐ den Leistungsumfang des Mietvertrags – unabhängig von einem konkreten Linienbündel.

(3) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung(en).

(4) Der vorliegende Vertrag tritt an die Stelle bisheriger Vereinbarungen der Vertragspartner zur Auftrags(daten)verarbeitung.

2. Konkretisierung des Auftragsinhalts, Zweck der Verarbeitung und Art der Daten

(1) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der bzw. den Leistungsvereinbarungen konkret beschrieben.

(2) Es geht dabei insbesondere um die Verarbeitung folgender Daten:

a) Erfassung von Unternehmen, Fahrernummer, Name und Vorname des Fahrers in einem Nutzerprofil (Fahrerdatensatz) zur Authentifizierung des Fahrers sowie zur Ermittlung von Qualitätsdaten. Hierbei werden Fahrtinformationen in Verbindung mit der Fahrernummer protokolliert, insbesondere zur Nachvollziehbarkeit von betrieblichen Ereignissen.

b) Darüber hinaus werden die Daten des Nutzerprofils zur betrieblichen Kommunikation im Rahmen der Verkehrssteuerung und -überwachung verwendet und bei ereignisbezogenen Meldungen betrieblich dokumentiert und digital weiterverarbeitet.

c) Die Vertriebsendgeräte (Fahrkartendrucker) werden über die Schnittstelle des VMS an das Hintergrundsystem des Auftragnehmers angebunden. Zum Zweck der Fahrerabrechnung werden die Verkaufsrohdaten im Hintergrundsystem des Auftragnehmers mit dem Fahrerdatensatz zusammengeführt. Die Daten der Fahrerabrechnung werden dem Auftraggeber zur kassentechnischen Abwicklung weitergeleitet.

d) Zur Aufklärung von betrieblichen oder sicherheitsrelevanten Vorfällen wird jeglicher Sprachfunkverkehr aufgezeichnet und im Bedarfsfall ausgewertet. Dies erfolgt auf Grundlage des berechtigten Interesses der Vertragspartner an der Aufklärung der genannten Vorfälle. Der Auftraggeber wird zusätzlich die Einwilligung seines Fahrpersonals zur Aufzeichnung des Sprachfunkverkehrs einholen und dem Auftragnehmer auf Verlangen vorlegen.

(3) Gegenstand der Verarbeitung personenbezogener Daten sind folgende **Datenarten und Datenkategorien**:

☒ Personenstammdaten (z.B. Name und Vorname)

☒ Fahrernummer und zugeordnetes Unternehmen

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

☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☐ Vertriebsdaten von Fahrkartenverkäufen

☒ Vertragsabrechnungs- und Zahlungsdaten

☐ Planungs- und Steuerungsdaten

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

☐ ……

(4) Folgende **Kategorien von Personen** sind von der Verarbeitung betroffen

☐ Kunden des Auftraggebers/Auftragnehmers

☒ Beschäftigte des Auftraggebers/Auftragnehmers

☐ Lieferanten des Auftraggebers/Auftragnehmers

☒ Ansprechpartner des Auftraggebers/Auftragnehmers

☐……

3. Technische und organisatorische Maßnahmen

(1) Die im **Anhang 1** dieses Vertrags beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem

Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Vertragspartnern zu vereinbaren.

(3) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber jederzeit auf Anforderung zu überlassen und kann auch durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Ort der Verarbeitung

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

6. Sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß der Artikel 28 - 33 DSGVO. Insofern gewährleistet er insbesondere die Einhaltung der in den folgenden Absätzen dargestellten Vorgaben.

(2) Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt: CTM-COM GmbH (www.ctm-com.de, datenschutz@ctm-com.de). Die aktuellen Kontaktdaten sind einsehbar unter https://heagmobilo.de/datenschutz. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

(3) Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der

in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(4) Der Auftraggeber und der Auftragnehmer arbeiten bei Anfragen der Aufsichtsbehörde vertrauensvoll zusammen. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(5) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

7. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieses Vertrags sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen (z.B. Telekommunikationsleistungen, Post - / Transport-Dienstleistungen). Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) grundsätzlich nur nach vorheriger dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftraggeber stimmt der Beauftragung der in **Anhang 2** (Genehmigte Unterauftragnehmer) genannten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Artikels 28 Absätze 2-4 DSGVO.

(3) Der Wechsel eines bestehenden Unterauftragnehmers ist zulässig, soweit der Auftragnehmer dem Auftraggeber eine angemessene Zeit vorab (mindestens sechs Wochen) in Textform den Wechsel anzeigt, der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer in Textform Widerspruch dagegen erhebt und auch mit dem neuen Unterauftragnehmer eine vertragliche Vereinbarung nach Maßgabe des Artikels 28 Absätze 2-4 DSGVO geschlossen wurde.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Absatz 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen (Textform) Zustimmung des Hauptauftraggebers. Sämtliche Regelungen sind in der Vertragskette auch dem weiteren Unterauftragnehmer aufzuerlegen.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Kontrollen vor Ort in Betriebsstätten des Auftragnehmers sind in der Regel rechtzeitig (mindestens 6 Wochen vor dem geplanten Termin) beim Auftragnehmer anzukündigen. Sie finden während der üblichen Betriebszeiten des Auftragnehmers statt (Montag – Freitag, 8-17 Uhr). Sofern der Kontrollumfang einen Werktag im Kalenderjahr überschreitet, kann der Auftragnehmer einen angemessenen Ausgleich seiner dafür anfallenden Kosten vom Auftraggeber verlangen.

(4) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz);

☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;

☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO.

9. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten und nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer einen angemessenen Ausgleich seiner dafür anfallenden Kosten vom Auftraggeber verlangen.

10. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Bestätigt der Auftraggeber die Weisung, so haftet er allein für alle daraus entstehenden Schäden, sollte sich nachträglich doch die datenschutzrechtliche Unzulässigkeit herausstellen.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

12. Haftung, Schlussbestimmungen

(1) Die Haftung der Vertragspartner richtet sich nach Artikel 82 DSGVO.

(2) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt.

(3) Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Vertragspartnern, insbesondere der Leistungsvereinbarung, gehen die Regelungen dieses Vertrags vor.

Ort, …….....

Verantwortlicher

....

Name

Darmstadt, ……..

Auftragsverarbeiter

..... …….....

Arne Rath Dirk Kornelius

Anhang 1: Technische und organisatorische Maßnahmen des Auftragnehmers

1. Zutrittskontrolle

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

☐ Alarmanlage	☐ Absicherung von Gebäudeschächten
☐ Automatisches Zugangskontrollsystem	☒ Chipkarten-/Transponder-Schließsystem
☐ Schließsystem mit Codesperre	☒ Manuelles Schließsystem
☐ Biometrische Zugangssperren	☒ Videoüberwachung der Zugänge
☐ Lichtschranken / Bewegungsmelder	☒ Sicherheitsschlösser
☒ Schlüsselregelung (Schlüsselausgabe etc.)	☒ Personenkontrolle beim Pförtner / Empfang
☒ Protokollierung der Besucher	☒ Sorgfältige Auswahl von Reinigungspersonal
☒ Sorgfältige Auswahl von Wachpersonal	☐ Tragepflicht von Berechtigungsausweisen

2. Zugangskontrolle

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

☒ Zuordnung von Benutzerrechten	☒ Erstellen von Benutzerprofilen
☒ Passwortvergabe	☐ Authentifikation mit biometrischen Verfahren
☒ Authentifikation mit Benutzername / Passwort	☒ Zuordnung von Benutzerprofilen zu IT-Systemen
☐ Gehäuseverriegelungen	☒ Einsatz von VPN-Technologie mit Multi-Faktor Authentifizierung
☐ Sperren von externen Schnittstellen (USB etc.)	☒ Sicherheitsschlösser
☒ Schlüsselregelung (Schlüsselausgabe etc.)	☒ Personenkontrolle beim Pförtner / Empfang
☒ Protokollierung der Besucher	☒ Sorgfältige Auswahl von Reinigungspersonal
☒ Sorgfältige Auswahl von Wachpersonal	☐ Tragepflicht von Berechtigungsausweisen
☒ Einsatz von Intrusion-Detection-Systemen	☒ Verschlüsselung von mobilen Datenträgern
☒ Verschlüsselung von Smartphone-Inhalten	☒ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
☒ Einsatz von Anti-Viren-Software	☒ Verschlüsselung von Datenträgern in Laptops / Notebooks
☒ Einsatz einer Hardware-Firewall	☒ Einsatz einer Software-Firewall

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.

- ☒ Erstellen eines Berechtigungskonzepts
- ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☐ physische Löschung von Datenträgern vor Wiederverwendung
- ☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☒ Verschlüsselung von Datenträgern
- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☒ Sichere Aufbewahrung von Datenträgern
- ☒ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- ☐ Protokollierung der Vernichtung

4. 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.

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☒ E-Mail-Verschlüsselung (selektiv)
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☒ Beim physischen Transport: sichere Transportbehälter/-verpackungen

5. 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.

- ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☒ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

6. Auftragskontrolle

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

- ☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☒ schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG
- ☒ Auftragnehmer hat Datenschutzbeauftragten bestellt
- ☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☐ Vertragsstrafen bei Verstößen
- ☐ vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Testen von Datenwiederherstellung
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☒ Klimaanlage in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuerlöschgeräte in Serverräumen
- ☐ Erstellen eines Backup- & Recoverykonzepts
- ☒ Erstellen eines Notfallplans
- ☒ Serverräume nicht unter sanitären Anlagen

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- ☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☒ Erstellung eines Berechtigungskonzepts
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☒ Festlegung von Datenbankrechten
- ☒ Logische Mandantentrennung (softwareseitig)
- ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- ☒ Trennung von Produktiv- und Testsystem

Anhang 2: Genehmigte Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers gemäß Ziffer 7 dieses Vertrags folgende Leistungen von Dritten in Anspruch:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Count+Care GmbH	Landwehrstraße 55 Darmstadt	IT-Dienstleistungen
Trapeze Switzerland GmbH	Rheinstrasse 36 Neuhausen Schweiz	Wartung und Pflege ITCS System
Nettropolis AG	Zeiloch 7 Bruchsal	Wartung und Pflege Nettro BME
IVU Traffic Technologies AG	Bundesallee 88 Berlin	Hintergrundsystem Fahrscheindrucker
vedisys AG	Dieselstr. 12 Griesheim	Vedisys QM und AmisData
Systemtechnik GmbH	Wielandstr. 12 Sömmerda	VAS (Vertriebs- und Abrechnungssystem)

(Stand: Juli 2025)