Vereinbarung zur Auftragsverarbeitung

Regelungen zu Datenschutz und Datensicherheit in Auftragsverhältnissen

Shiftmove GmbH
Warschauer Straße 57
10243 Berlin

- nachfolgend Auftragsverarbeiter" genannt -

und Ihnen

- nachfolgend „Verantwortlicher" genannt -

- nachfolgend gemeinsam „Vertragsparteien" genannt -

Präambel

Dieser Auftragsverarbeitungsvertrag ("AVV") gem. Art. 28 DSGVO ist Teil unserer Allgemeinen Geschäftsbedingungen ("Hauptvertrag"), die zwischen unseren Kund:innen und der Shiftmove GmbH geschlossen wurden und hier aufrufbar sind: https://www.shiftmove.com/legal/agb. Gemäß dieser Vereinbarung findet dieser AVV Anwendung auf die Verarbeitung Ihrer personenbezogenen Daten im Rahmen der Bereitstellung unseres Produkts.

Mit Unterzeichnung des Bestellformulars gelten die AGB einschließlich dieses AVV als verbindlich vereinbart, sodass eine gesonderte Unterzeichnung dieses AVV grundsätzlich nicht erforderlich ist.

Gleichwohl stellen wir unseren Kund:innen die Möglichkeit bereit, den AVV separat herunterzuladen, zu unterzeichnen und uns zukommen zu lassen. In diesem Fall bitten wir darum, eine Kopie der unterzeichneten Version an **privacy@shiftmove.com** zu senden.

Die Vereinbarung orientiert sich an den Regelungen der DSGVO, dem BDSG und dem Data Act.

§ 1 Gegenstand des Auftrags; Art und Zweck der Verarbeitung; Art der personenbezogenen Daten, Kategorien betroffener Personen

(1) Der Gegenstand des Auftrags ist die Bereitstellung von Software-as-a-Service-Dienstleistungen aus dem Angebot der Shiftmove Gruppe („Services“). Gegenstand und Zweck der Verarbeitung werden weiterhin in Anlage 1a genauer definiert. Die Art der Verarbeitung ist in Anlage 1b definiert.

(2) Die Kategorien betroffener Personen sind in Anlage 1c definiert.

(3) Die Art der verarbeiteten personenbezogenen Daten sind in Anlage 1d definiert.

(4) Anlage 1 ist Bestandteil dieser Vereinbarung.

(5) Der Verantwortliche weist den Auftragsverarbeiter zur Verarbeitung dieser Daten zu diesen Zwecken an.

§ 2 Dauer des Auftrages

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages.

§ 3 Verantwortlichkeit und Weisungsbefugnis

(1) Der Verantwortliche ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO). Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke als in dieser Auftragsverarbeitungsvereinbarung und in dem Hauptvertrag festgelegt und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Etwas Anderes gilt nur in dem in Absatz 2 genannten Umfang.

(2) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn es besteht eine anderweitige Verpflichtung durch Unionsrecht oder dem Recht des Mitgliedsstaates, dem der Auftragsverarbeiter unterliegt. Im Falle einer anderweitigen Verpflichtung teilt der Auftragsverarbeiter dem Verantwortlichen vor der Verarbeitung unverzüglich die entsprechenden rechtlichen Anforderungen mit.

(3) Der Verantwortliche, nicht aber der Auftragsverarbeiter, ist Dateninhaber (vgl. Erwägungsgrund 22 zum Data Act). Der Auftragsverarbeiter sichert zu, alle vom Verantwortlichen übermittelten Daten (personenbezogene und nicht-personenbezogene Daten) nicht für eigene Zwecke, zur Profilbildung oder zur Produktverbesserung zu nutzen, es sei denn, es wurde dem Auftragsverarbeiter ausdrücklich gestattet. Der Auftragsverarbeiter erfüllt damit die Anforderungen aus Art. 6 und Art. 8 Abs. 2 Data Act.

(4) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DSGVO unverzüglich den

Verantwortlichen. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragsverarbeiter berechtigt, die Durchführung der Weisung auszusetzen.

(5) Änderungen des Verarbeitungsgegenstands mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen.

§ 4 Vertraulichkeit

Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO auf die Vertraulichkeit verpflichtet worden sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten einschließlich der in diesem Auftragsverarbeitungsvertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

§ 5 Datensicherheit

(1) Die Vertragsparteien vereinbaren die in der Anlage 2 „Technische und organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(2) Anlage 2 ist Bestandteil dieser Vereinbarung.

(3) Der Auftragsverarbeiter beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Verantwortlichen schriftlich mitzuteilen.

(4) Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß Art. 33, 34 DSGVO nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

(5) Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

- eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
- Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
- die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

§ 6 Einbeziehung weiterer Auftragsverarbeiter (Subunternehmer)

(1) Als Subunternehmer im Sinne dieser Regelung sind weitere Auftragsverarbeiter zu verstehen, deren Dienstleistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen und Reinigung in Anspruch nimmt. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Einsatz von Subunternehmer oder der Wechsel des bestehenden Subunternehmers sind zulässig, soweit:

- der Auftragsverarbeiter eine solche Auslagerung auf Subunternehmer dem Verantwortlichen 14 Kalendertage vorab schriftlich oder in Textform anzeigt und
- der Verantwortliche nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt.

(3) Sollte der Verantwortliche einer Änderung eines Subunternehmers innerhalb der zugestanden Widerspruchsfrist nach § 6 Abs. 2 widersprechen, wird der Auftragsverarbeiter prüfen und dem Verantwortlichen mitteilen, ob eine Bereitstellung der Dienstleistung ohne die Änderung des Subunternehmers möglich ist. Wenn der Auftragsverarbeiter die Dienstleistung entsprechend seiner Prüfung nicht ohne die Änderung des Subunternehmers erbringen kann, so haben beide Vertragsparteien das Recht, den Vertrag schriftlich mit einer Frist von 14 Tagen zu kündigen.

(4) Mit dem Subunternehmer ist eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 3 und 4 DSGVO abzuschließen.

(5) Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Subunternehmer und dessen erstmaliges Tätigwerden ist erst mit Vorliegen aller gesetzlichen Voraussetzungen für eine Unterbeauftragung gestattet. Die durch den Verantwortlichen zum Zeitpunkt des Vertragsschlusses genehmigten Subunternehmer sind in Anlage 3 genannt. Weiterhin können die Dienstleister der jeweiligen Subdienstleister unter folgenden Links https://www.vimcar.de/legal/danteschutz/subunternehmer und https://www.avrios.com/legal/sub-processors eingesehen werden.

(6) Verbundene Unternehmen der Shiftmove Gruppe sind als Subunternehmer beauftragt, soweit sie in den Listen unter § 6 Abs. 4 dieser Vereinbarung genannt sind.

(7) Jede Verlagerung der Datenverarbeitung in ein Drittland bedarf der vorherigen dokumentierten Weisung des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO) und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44-49 DSGVO erfüllt sind.

(8) Anhang 3 ist Bestandteil dieser Vereinbarung.

§ 7 Betroffenenrechte

(1) Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, den Pflichten zur Beantwortung von Anträgen auf Wahrung der in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen nachzukommen (Art. 28 Abs. 3 S. 2 lit. e DSGVO).

(2) Soweit die betroffene Person gegenüber dem Verantwortlichen ein Recht auf Datenübertragbarkeit besitzt, stellt der Auftragsverarbeiter sicher, dass der Verantwortliche die im Verantwortungsbereich des Auftragsverarbeiters verarbeiteten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format erhalten kann.

(3) Der Auftragsverarbeiter darf personenbezogene Daten nur nach dokumentierter Weisung des Verantwortlichen herausgeben, berichtigen, löschen oder deren Verarbeitung einschränken (Art. 28 Abs. 3 S. 2 lit. g DSGVO).

(4) Soweit eine betroffene Person sich unmittelbar an den Auftragsverarbeiter wendet, um ihre Rechte gemäß Art. 12 bis 22 DSGVO geltend zu machen, wird der Auftragsverarbeiter das Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(5) Auskünfte an Dritte oder den betroffenen Personen darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen.

(6) Der Verantwortliche ist dafür verantwortlich Betroffene im Rahmen der Art. 12 und 13 DSGVO zu informieren. Erforderliche Informationen, die im Zusammenhang mit dieser Pflicht stehen und über die nur der Auftragsverarbeiter verfügt, wird dieser dem Verantwortlichen auf Anfrage zur Verfügung stellen.

(7) Der Auftragsverarbeiter wird den Verantwortlichen auf dessen Aufforderungen dabei unterstützen, Daten in einem strukturieren, interoperablen und maschinenlesbaren Format

bereitzustellen und ggfs. an Dritte weiterzugeben, soweit der Verantwortliche als Dateninhaber von Nutzern nach Art. 4ff. und Art. 8 Data Act in Anspruch genommen wird.

§ 8 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags die gesetzlichen Pflichten gemäß Art. 28 bis 36 DSGVO zu beachten. Insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Ist der Auftragsverarbeiter nach Art. 37 DSGVO, § 38 BDSG gesetzlich dazu verpflichtet, einen Datenschutzbeauftragten schriftlich zu benennen, so teilt der Auftragsverarbeiter dem Verantwortlichen die Kontaktdaten des Datenschutzbeauftragten zum Zwecke der direkten Kontaktaufnahme mit. Ein Wechsel des Datenschutzbeauftragten ist bei dem Verantwortlichen unverzüglich anzuzeigen.

- Als externe Datenschutzbeauftragte ist beim Auftragsverarbeiter

  clever datenschutz GmbH
  E-Mail: privacy@shiftmove.com

  bestellt.

(2) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in Art. 32 - 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Hierzu gehören insbesondere

- 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
- die Verpflichtung, den Verantwortlichen unverzüglich zu informieren, wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird (Art. 28 Abs. 3 lit. f, Art. 33 Abs. 2 DSGVO);
- die Verpflichtung, dem Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
- die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzung;
- die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(3) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich unter Einhaltung der gesetzlichen Anforderungen zur Übermittlung von Daten in Drittländer gem. Art. 44ff. DSGVO. Der Auftragsverarbeiter wird zur Sicherstellung eines angemessenen Datenschutzniveaus lediglich Daten an Empfänger in Drittländern übermitteln, insofern für das betreffende Drittland ein Angemessenheitsbeschluss der EU-Kommission besteht (Art. 45 DSGVO), angemessene Garantien für die Übermittlung vorliegen, etwa Standardvertragsklauseln, (Art. 46 DSGVO), interne Datenschutzvorschriften vorliegen (Art. 47 DSGVO) oder sonstige Ausnahmetatbestände für die Übermittlung von Daten vorliegen (Art. 48 DSGVO). Der Verantwortliche stimmt der Übermittlung von Daten an die ggf. in Drittländern ansässigen Subunternehmen aus § 6 Abs. 5 dieser Vereinbarung zu.

(4) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Pflichten zur Datenportabilität und beim Anbieterwechsel gemäß den Anforderungen des Data Act und gibt Hinweise zu unterstützten Formaten und Schnittstellen gem. Art. 23- 29 Data Act.

§ 9 Kontrollrechte des Verantwortlichen, Art. 28 Abs. 3 S. 2 lit. h DSGVO

(1) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle im schriftlichen Verfahren erforderlich sind.

(2) Der Verantwortliche hat das Recht, sich vor Beginn der Verarbeitung sowie regelmäßig von der Einhaltung der beim Auftragsverarbeiter umgesetzten technischen und organisatorischen Maßnahmen zu überzeugen.

Dies erfolgt in erster Linie durch:

- die Einholung von Auskünften des Auftragsverarbeiters und/oder
- die Vorlage unabhängiger Prüfberichte oder anerkannter Zertifizierungen.

a) Anlassbezogene Vor-Ort-Kontrollen

Der Verantwortliche ist berechtigt, eine Vor-Ort-Kontrolle beim Auftragsverarbeiter durchzuführen, wenn:

- konkrete Anhaltspunkte für Zweifel an der Richtigkeit oder Vollständigkeit der vorgelegten Prüfberichte oder Zertifizierungen bestehen,
- ein Sicherheitsvorfall im Sinne des Art. 33 Abs. 1 DSGVO im Zusammenhang mit der Datenverarbeitung aufgetreten ist, oder
- die zur Verfügung gestellten Unterlagen die erforderlichen Nachweise nicht vollständig erbringen.

Vor-Ort-Kontrollen sind in diesen Fällen grundsätzlich mindestens 14 Kalendertage vorher schriftlich anzukündigen.
Eine Verkürzung dieser Frist ist nur in begründeten Ausnahmefällen zulässig, wenn die Dringlichkeit sich unmittelbar aus dem jeweiligen Anlass ergibt (z. B. bei einem

Sicherheitsvorfall). In diesem Fall hat der Verantwortliche die Gründe für die verkürzte Frist nachvollziehbar darzulegen und auf Verlangen gegenüber dem Auftragsverarbeiter zu belegen.

b) Anlasslose Vor-Ort-Kontrollen

Unabhängig von einem konkreten Anlass kann der Verantwortliche einmal pro Kalenderjahr eine anlasslose Vor-Ort-Kontrolle durchführen. Auch anlasslose Vor-Ort-Kontrollen sind durch den Verantwortlichen mindestens 14 Kalendertage vorher schriftlich anzukündigen.

c) Allgemeine Rahmenbedingungen

Die Ausübung des Kontrollrechts darf den Geschäftsbetrieb des Auftragsverarbeiters nicht unangemessen stören oder missbräuchlich erfolgen.
Die tatsächlich entstehenden Kosten anlassloser Vor-Ort-Kontrollen trägt der Verantwortliche.

(3) Der Verantwortliche ist verpflichtet, über jede durchgeführte Kontrolle ein Protokoll anzufertigen. Sämtliche im Rahmen der Kontrolle festgestellten Abweichungen, Mängel oder sonstigen wesentlichen Feststellungen sind dem Auftragsverarbeiter unverzüglich, in jedem Fall jedoch innerhalb einer angemessenen Frist nach Abschluss der Kontrolle in Textform mitzuteilen. Das Protokoll ist dem Auftragsverarbeiter auf Anforderung zur Verfügung zu stellen.

§ 10 Haftung

(1) Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Eine Haftung des Auftragsverarbeiters gegenüber dem Verantwortlichen wegen Verletzung von Pflichten aus diesem Vertrag oder dem Hauptvertrag bleibt hiervon unberührt.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. § 10 Abs. 2 Satz 1 gilt im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

§ 11 Kündigung und Beendigung des Auftrages (Art. 28 Abs. 3 S. 2 lit. g DSGVO)

(1) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

(2) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn:

- Der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
- der Auftragsverarbeiter fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen aus der Datenschutz-Grundverordnung verletzt.
- der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln oder der Datenschutz-Grundverordnung zum Gegenstand hat, nicht nachkommt.

(3) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

(4) Der Auftragsverarbeiter hat nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Verantwortlichen alle personenbezogenen Daten entweder zu löschen oder zurückzugeben, sofern nicht nach einer gesetzlichen Norm eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht oder der Verantwortliche einen Zugang nach Ziff. 2.1.5 der AGB verlangt.

(5) Der Auftragsverarbeiter bestätigt dem Verantwortlichen in diesem Falle mit Datumsangabe in Textform ohne weitergehende Aufforderung, dass er sämtliche ihm gegebenenfalls überlassenen Datenträger sowie sonstigen Unterlagen an den Verantwortlichen herausgegeben oder vernichtet bzw. sicher gelöscht und somit keine Daten des Verantwortlichen zurückbehalten hat.

(6) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 12 Schlussbestimmungen

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(2) Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrerer Regelungen werden die Vertragsparteien die unwirksame Regelung unverzüglich durch eine solche Regelung ersetzen, die der unwirksamen Regelung wirtschaftlich und datenschutzrechtlich am ehesten entspricht.

(3) Die Vertragsparteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(4) Mündliche Nebenabreden zwischen den Parteien bestehen nicht. Jede Änderung, Ergänzung oder Aufhebung dieser Vereinbarung bedarf zu ihrer Wirksamkeit der Schriftform, auf die nur schriftlich verzichtet werden kann. Für die Wahrung der Schriftform genügt jeweils eine Unterzeichnung mit mindestens einfacher elektronischer Signatur mit Protokollierung mittels einer e-Signatur-Software. Der elektronischen Signatur kommt volle Beweiskraft zu.

(5) Soweit andere Vereinbarungen zum Zeitpunkt des Abschlusses dieses Vertrages anderslautende oder diesem Vertrag widersprechende Angaben enthalten, so gehen die Inhalte dieses Vertrages vor.

(6) Die folgenden Anlagen sind Bestandteil dieser Vereinbarung: Anlage 1 „Informationen zur Verarbeitung“, Anlage 2 „Technische organisatorische Maßnahmen“, Anlage 3 “Subunternehmer”.

Unterschrift

Firma:	
Anschrift	
Datum:	
Ort:	
Name:	
Unterschrift Verantwortlicher	

Firma:	Shiftmove GmbH
Anschrift	Warschauer Str. 57, 10243 Berlin
Datum:	15.09.2025
Ort:	Berlin
Name:	i.V. John Maik Ryssel
	Signed by: i.V. John Maik Ryssel 4ABB00F788844C5...
Unterschrift Auftragsverarbeiter	

Anlage 1

Informationen zur Verarbeitung

Die nachstehend aufgeführten Informationen zu Gegenstand und Zweck der Verarbeitung, zu den Arten der Verarbeitung, zu den Kategorien betroffener Personen sowie zu den Kategorien verarbeiteter personenbezogener Daten beziehen sich auf den gesamten möglichen Funktionsumfang der vom Auftragsverarbeiter angebotenen Services. Verbindlich sind ausschließlich diejenigen Zwecke, Verarbeitungsarten, Betroffenen- und Datenkategorien, die sich aus dem Hauptvertrag einschließlich der jeweils vereinbarten Order Form / Bestellformular ergeben und die für die tatsächlich vom Verantwortlichen bestellten Produkte und Funktionen erforderlich sind.

a) Gegenstand und Zweck der Verarbeitung

- Software für Flottenmanagement (Avrios) inklusive der folgenden Zwecke:
  - Verwaltung von Fahrzeugen und Fahrern
  - Verwaltung von Bußgeldbescheiden
  - Verwaltung von Tankkarten
  - Verwaltung von Schadensmeldungen
  - Durchführung von Führerscheinkontrollen
  - Erstellung von Reports und Analysen

- Live-Ortung und Routendokumentation (Vimcar Fleet Geo) inklusive der folgenden Zwecke:
  - Live-Ortung von Fahrzeugen
  - Routendokumentation von Fahrzeugen
  - Geo-Fencing Benachrichtigung für Fahrzeuge

- elektronisches Fahrtenbuch (Fahrtenbuch) inklusive der folgenden Zwecke:
  - Routendokumentation von Fahrzeugen
  - Export von Fahrtenbuchdaten

b) Art der Verarbeitung

Im Rahmen der Beauftragung wird der Auftragsverarbeiter folgende Arten der Verarbeitung nach Art. 4 Nr. 2 DSGVO: Erhebung, Erfassung, Organisation, Ordnung, Speicherung, Anpassung, Veränderung, Auslesen, Abfragen, Übermittlung, Einschränkung, Löschung und Vernichtung von Daten.

c) Kategorien der Betroffenen und personenbezogener Daten

Bei der Bereitstellung der Services können regelmäßig personenbezogene Daten folgender Kategorien von Betroffenen verarbeitet werden:

1) Fahrer (ehemalige und aktuelle Mitarbeiter und deren Ehepartner und Angehörige, aktuelle Auftragnehmer sowie Bewerber und zukünftige Mitarbeiter);
2) Benutzer (autorisierte Benutzer des Kunden (die keine Fahrer sind), die zur Nutzung der Dienstleistungen berechtigt sind);
3) Dritte (Kunden, Geschäftspartner, Lieferanten, Berater, Vertreter, Freiberufler und/oder Subunternehmer des Kunden (natürliche Personen)).

d) Art der verarbeiteten Daten

Bei der Nutzung unserer Produkte werden, je nach Umfang und individueller Nutzung, die folgenden Kategorien von Daten verarbeitet werden:

Flottenmanagement Avrios:

- Aufgaben und Kommentare
- Bußgeldbescheidinformationen (Adressat, Höhe, Fotos)
- Eintrittsdatum und Austrittsdatum
- Fahrzeuginformationen (CO2-Ausstoß, Schadensmeldungen, Nummernschild, Fahrgestellnummer)
- Fotos (Führerscheinfotos und Portraitfotos)
- Führerscheininformationen
- Kontaktinformationen (Telefonnummer, Faxnummer, Mobiltelefonnummer, E-Mail-Adresse)
- Kommunikationsverläufe (E-Mail-Verläufe mit Zulieferern, Dienstleistern, Versicherungen etc.)
- Personenstammdaten (Vorname, Nachname, Adresse, Geschlecht, Geburtsdatum und -ort, Sprache, Nationalität, Aufenthaltsberechtigung, Zivilstand, Angaben zu Angehörigen, nationale Identifikationsnummer)
- Unternehmensverwaltungsdaten (interne ID, Kostenstelle, Organisation, Abteilung, Standort, Branche und Teilbranche, Berichtsstruktur)
- Informationen zur Lohnplanung (Nebenleistungen rund um Firmenwagen), Leistungsverzeichnisse und zugehörige Informationen (Anspruch auf Firmenwagen und Klasse des Firmenwagens)
- Tankkarteninformationen (Anbieter, Kosten, Datum, Produkt)

- Unfallverhütungsvorschrift-Testergebnisse
- Gerätedaten und IT-Nutzungsdaten

Vimcar Fleet Geo:

- Vorname, Nachname
- E-Mail-Adresse, Telefonnummer, Mobiltelefonnummer
- Fahrtenbuchdaten
- Fahrtdaten während der Fahrt
- Live-Ortung und Routendokumentation;
- VIN (Vehicle Identification Number)
- Prüfparameter für die Durchführung der automatisierten Führerscheinkontrolle (optional bei Nutzung der Führerscheinkontrolle)
- Technische Fahrzeugdaten (z.B. Reparaturstatus), Fotos von Fahrzeugen (optional bei der Nutzung des Schadensmanagements
- Tankkarteninformationen (Anbieter, Kosten, Datum, Produkt)
- Fahrzeugbuchungen (Datum, Fahrzeug, Dauer, Fahrer:in)
- Gerätedaten und IT-Nutzungsdaten

Vimcar Fahrtenbuch:

- Vorname, Nachname
- E-Mail-Adresse, Telefonnummer, Mobiltelefonnummer
- Fahrtenbuchdaten
- Fahrtdaten während der Fahrt
- Start- und Endpunkt von Touren
- gefahrene Kilometer
- Kategorisierung von Privat- und Geschäftsfahrten
- Kontakt- und Adressdaten
- VIN (Vehicle Identification Number)
- Prüfparameter für die Durchführung der automatisierten Führerscheinkontrolle (optional bei Nutzung der Führerscheinkontrolle)
- Technische Fahrzeugdaten (z.B. Reparaturstatus), Fotos von Fahrzeugen (optional bei der Nutzung des Schadensmanagements
- Gerätedaten und IT-Nutzungsdaten

Anlage 2

Technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO der Shiftmove GmbH

1. Maßnahmen zu Gewährleistung der Vertraulichkeit

1.1 Zutrittskontrolle

Beschreibung: Soll verhindern, dass Unbefugte räumlich Zugang zu Datenverarbeitungsanlagen erhalten. Maßnahmen zur Gebäude- und Raumsicherung.

- Allgemeines (dokumentiertes) Gebäudesicherungskonzept
- Schließsystem/ Schließanlage
- Einbruchshemmende Fenster & Türen
- Externer Wachdienst
- Alarmanlage
- Verbindung Alarmanlage zu Wachdienst/ Polizei
- Lichtschranken/ Bewegungsmelder
- Verbindung Bewegungsmelder zu Wachdienst/ Polizei
- Videoüberwachung
- (konkretes) Zutrittsberechtigungskonzept
- Biometrische Zutrittskontrolle
- Personenüberprüfung bei Pförtner /Empfang
- Protokollierung von Besucherzutritten / Besucherbuch
- Begleitung von externen Personen in Sicherheitsbereichen
- Besucherausweise
- Elektronische Zutrittscodekarten/ Zutrittstransponder
- Sicherheitszonen (Besucherbesprechung, Serverräume, Arbeitsplätze, Forschung)
- Bestehen einer Berechtigungsübersicht zu den Sicherheitszonen
- Bei Zonenübergang werden selbstschließende Türen eingesetzt
- Berechtigungsausweise (für einzelne Zonen)
- Schlüsselregelung
- Gesondert gesicherter Eingang für An- und Ablieferungen
- Gesondert gesicherter Zutritt zum Serverraum
- Gesondert gesicherter Zutritt zum Rechenzentrum
- Sorgfältige Auswahl von Reinigungspersonal
- Arbeitsanweisungen /Richtlinien bzgl. des Verschließens von Räumlichkeiten bei Verlassen/Arbeitsende

1.2 Zugangskontrolle

Beschreibung: Soll den Zugang Unbefugter zu Datenverarbeitungssystemen und deren unbefugte Nutzung verhindern.Systemabsicherung.

- Rollenkonzept / Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Berechtigungsmanagement
- Vermeidung von Gruppenkennungen
- Dokumentierter Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern
- Dokumentierter Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern
- Dokumentierter Prozess zum Rechteentzug bei Austritt von Mitarbeitern
- Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen
- Verwendung von individuellen Passwörtern
- Login mit Benutzername und Passwort
- Login mit biometrischen Daten
- Separates BIOS-Passwort
- Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)
- Blickschutzfolien bei potenzieller unbefugter Einsichtnahme
- Passwortrichtlinie mit Mindestvorgaben zur Passwortkomplexität:
    - Mindestens 8 Zeichen
    - Mindestens 12 Zeichen für lokale Admin-Passwörter
    - Groß- und Kleinschreibung, Sonderzeichen, Zahl (davon mind. 4 Kriterien)
    - Verhinderung von Trivialpasswörtern (z.B. Passwort1, Passwort2, 123456, qwertz)
    - Passworthistorie (kein erneute Verwendung der letzten Passwörter)
    - Verhinderung von PW nach positivem Abgleich mit Wörterbüchern
    - Eingabebeschränkung bestimmter Sonderzeichen zur Verhinderung von SQL-Injections
    - Angemessen sicheres Verfahren zum Zurücksetzen von PW
- Zeitverzögerung zwischen einzelnen Login-Versuchen
- Fehlgeschlagene Anmeldeversuche werden Nutzern angezeigt
- Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von PW
- Sperrung Passwörter nach Sicherheitsvorfall und Neuvergabe
- Sperrung Passwörter bei Verdachtsfall
- Weitgehend automatische (technische) Umsetzung der Passwortrichtlinie
- Zwei- oder Mehrfaktorauthentifizierung bei Verarbeitungen mit hohem Risiko
- Speichern v. Passwörtern im Browser nur mit Masterpasswort
- Zugang zu Websites wird restriktiv verwaltet
- Sonstiges: (z.B. Nutzung von Fido2)
- Hashing von gespeicherten Passwörtern mittels aktueller Hash-Verfahren:
    - Genutztes Hashverfahren:
    - Hashes werden „gesalzen“ (Salt) oder „gepfeffert“(Pepper)
- Verschlüsselung von Netzwerken
    - Verwendete Verschlüsselungsalgorithmen: SSH, HTTPS, TLS 1.2+,

- Verschluss von Datenverarbeitungsanlagen (z.B. verschlossener Cage für Server)
- Sperrung von externen Schnittstellen (z.B. USB)
- Verwendete Verschlüsselungsalgorithmen:
- Deaktivierung des Auto-Starts externer Medien
- Programmprüfungs- und Freigabeverfahren bei Neuinstallationen
- Verhinderung der Ausführung von heruntergeladener Software, deren Quellen als unsicher gekennzeichnet werden
- Verhinderung automatischer Ausführung v. Programmen aus temporären Downloads
- Verwendung von Intrusion-Prevention-Systemen
- Nutzung von VPN-Technologie
- Einsatz von Anti-Viren-Software: Server
- Einsatz von Anti-Viren-Software: Clients
- Einsatz einer Software-Firewall
- Einsatz einer Hardware-Firewall
- Zentrale Erfassung von Schadcode-Alarmmeldungen
- Standard-Authentifizierungsinformationen werden nach Softwareinstallation/erstem Login geändert
- Zentrale Geräteverwaltung
- Mobile-Device-Management
- Bei Smartphone: Zugang nur nach Authentifizierung
- Bei Smartphone: Einsatz biometrischer Zugangsverfahren nur bei ausschließlich lokaler Speicherung der biometrischen Templates (innerhalb Secure-Chips)
- Bei Smartphone: Sichere Quellen für Apps, Apps werden getestet und freigegeben
- Aufbewahrung personenbezogener Daten/Datenträgern in verschließbaren Sicherheitsschränken oder in gesondert gesicherten Räumen
- Regelung zum Home Office / zu Telearbeit
- Regelung zur Privatnutzung v. Geräten oder Ausschluss der Privatnutzung
- Sonstige Maßnahmen:
    - Verschiedene Passwörter für verschiedene Dienste oder SSO
    - Verwendung eines Passwortmanagers

1.3 Zugriffskontrolle

Beschreibung: Soll unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen verhindern.

- Nutzung eines Berechtigungskonzepts
- Minimaler Einsatz von Administratoren-Konten
- Verschiedene administrative Rollen nach least Privilege-Konzept (Benutzer, Firewall, Backups etc.)
- Superuser (z.B. root unter Linux) soweit möglich nicht verwendet
- Regelung, dass nicht unter Nutzung von Administratorenrechten im Internet gesurft oder E-Mails gelesen/versendet werden darf
- Verwendung eigener Administrations-Endgeräte (dedizierte Netzwerkverbindung)
- Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)
- Versendung von Telemetriedaten an Hersteller deaktiviert
- Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)

- Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) im zutrittsgeschützten Safe
- Regelmäßige Überprüfung von Rollen und Berechtigungen
- Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken
- Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)
- Regelmäßige Auswertung von Protokollen (Logfiles)
- Zeitliche Begrenzung von Zugriffsmöglichkeiten
- Deaktivierung v. ungenutzten Standard Server-Diensten
- Protokollierung auf Firewall-Ebene, um unbefugte Zugriffe zwischen den Netzten festzustellen
- Automatische Benachrichtigungen bei Verdacht auf unbefugte Verarbeitungen
- Protokollierung von Fernwartungszugriffen
- Protokollierung von Dateizugriffen
- Protokollierung von Dateilöschungen
- Protokollierung von Dateiveränderungen
- SPAM-Filter
- Intrusion-Detection (IDS)
- Software für das Security Information and Event Management (SIEM)
- Instrusion-Prevention (IPS)
- Beschränkter Zugriff auf LogFiles (nur Log-Admin)
- Speicherung von Log-Files auf dediziertem LogFile-Server
- Verschlüsselte Speicherung der Daten
- verwendete Verschlüsselungsalgorithmen:
    - AES (128/256 bit)
    - 3DES
    - RSA (1024/2048 bit)
    - EC (256 bit)
    - Sonstiges: AES 256 AWS at rest Verschlüsselung
- Verwendete Hash-Funktion:
    - SHA2 (256, 384, 512 bit)
    - SHA3
    - bcrypt
- Andere Verfahren:
    - Hashes werden „gesalzen“ (Salt) oder „gepfeffert“(Pepper)
- Zwei-Faktor-Authentifizierung zur Wartung von Webservern
- SSL Zertifikate nur aus vertrauenswürdigen Stellen
- Kontrollierte Vernichtung von Daten:
    - Datenträgerentsorgung - Sichere Löschung von Datenträgern (DIN 66399)
    - Shredder (Cross-Cut, at least level 3, DIN 66399)
    - Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleister
    - Peter-Gutmann-Algorithmus – 35-faches Überschreiben
    - Physikalische Zerstörung (z.B. Shredder bei Partikelgrößen bis max. 1000 Quadrat-Millimeter)
    - Entmagnetisierung durch thermische Zerstörung (Erhitzung der Magnetplattenoberfläche über die Curie-Temperatur der verwendeten Beschichtung hinaus)
    - Entmagnetisierung mittels eines Degaussers

- Anbindung von Niederlassungen oder Homeoffice nur über VPN-Verbindungen mit Client-Zertifikatsauthentifizierung
- Einsatz von WLAN nur auf aktuellen Routern mit wirksamen Zugangsmechanismen
- WLAN-Gastzugang ohne Zugriff auf internes Netzwerk
- Richtlinie zur Datenvernichtung
- Clean Desk-Policy
- Prüfung eingehender E-Mails mittels Anti-Malware
- Sicherheitskonzept für den Umgang mit Druckern, Kopierern etc.
- Sonstige Maßnahmen:
- Schlüsselverwaltung über Hardware Security Module

2. Maßnahmen zur Gewährleistung der Integrität

2.1 Weitergabekontrolle

Beschreibung: Soll die Sicherheit der Daten bei elektronischer Übertragung und Datentransport und die Nachvollziehbarkeit der Weitergabe gewährleisten.

- Wie werden Daten zwischen an Dritte übermittelt?
  - VPN-Verbindung
  - Secure File Transfer Protocol (sftp)
  - Citrix-Verbindung
  - TLS 1.2+
- E-Mail-Verschlüsselung
  - E-Mail-Versand mit verschlüsselten ZIP-Dateien
- Bei Messengern: Transport- und Inhaltsverschlüsselung
- Datenaustausch über https-Verbindung
- verwendetes Verschlüsselungsprotokoll:
  - TLS 1.2
  - TLS 1.3
- Sonstige Versendungsart:
- verwendete Verschlüsselungsalgorithmen:
  - AES (128/256 bit)
  - 3DES
  - RSA (1024/2048 bit)
  - Diffie-Hellmann
- Nutzung von Signaturverfahren
- Verwendetes Signaturverfahren:
  - RSA
  - ElGamal
  - DSA
- Digitales Signieren von Makros

- Keine Übertragung personenbezogener Daten (z. B.Mail-Adresse) per HTTP-GET-Request, da diese in den Webserver-Log-Dateien gespeichert werden und durch eingesetzte Website-Tracker ausgeleitet werden können
- Bei HTTPS: Einsatz von Client-Zertifikaten
- Verschlüsselte Anfragen an DNS-Dienste
- Regelung zur Nutzung von Cloud-Diensten (inkl. Exit-Strategie)
- Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle
- Verschlüsselung vertraulicher Datensätze
- Verschlüsselung mobiler Datenträger (z.B. Laptop-Festplatten, externe Festplatten, USB-Sticks)
- Verbot der Mitnahme von Taschen und sonstigen Gepäckstücken sowie Mobiltelefonen in Sicherheitsbereiche
- Regelung zur Anfertigung von Datensatz-Kopien
- Erstellen von Sicherungskopien von Datenträgern, die transportiert werden müssen
- Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege
- Direktabholung, Kurierdienst, Transportbegleitung
- Vollständigkeits- und Richtigkeitsprüfung

2.2 Eingabekontrolle

Beschreibung: Soll gewährleisten, dass nachvollzogen werden kann, ob, wer, wann personenbezogene Daten in Datenverarbeitungssysteme eingeben, geändert oder gelöscht hat.

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Manuelle oder automatisierte Auswertung der Protokolle
- Differenzierte Benutzerberechtigungen:
    - Einzelne Benutzernamen, keine Benutzergruppen
    - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
    - Feldzugriff bei Datenbanken
- Organisatorische Festlegung von Eingabezuständigkeiten
- Verpflichtung auf das Datengeheimnis
- Über OS-Standard hinausgehendes Log-Konzept
- Dezidierter Logserver
- Regelung der Zugriffsberechtigungen für Logserver (LogAdmin)
- Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke

3. Maßnahmen zur Gewährleistung der Verfügbarkeit & Belastbarkeit

3.1 Verfügbarkeitskontrolle

Beschreibung: Soll Daten gegen zufällige Zerstörung oder Verlust schützen.

- Brandmeldeanlagen in Serverräumen
- Rauchmelder in Serverräumen
- Brandschutztüren
- Wasserlose Brandbekämpfungssysteme in Serverräumen
- Wassersensoren in Serverräumen
- Blitz-/ Überspannungsschutz
- Klimatisierte Serverräume
- Serverräumlichkeiten in separaten Brandabschnitt
- Unterbringung von Backupsystemen in separaten Räumlichkeiten und in separatem Brandabschnitt
- Serverräume nicht unter oder neben sanitären Anlagen
- Zutrittsbegrenzung bei Serverräumen auf notwendiges Personal
- Alarmmeldung bei unberechtigten Zutritt zu Serverräumen
- Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)
- CO2-Feuerlöscher in unmittelbarer Nähe der Serverräume
- USV-Anlage (Unterbrechungsfreie Stromversorgung)
- Stromgenerator
- Feuerfeste Schränke
- Datenschutztresor
- Dokumentiertes Datensicherungs- und Backupkonzept
- Durchführung von Datensicherungen und Erstellen von Backups nach 3-2-1-Prinzip
- Havariearchiv (Auslagerung von Daten)
- Regelmäßige Tests zur Datenwiederherstellung
- Mindestens ein Backup-System ist durch Schadcode nicht verschlüsselbar
- Spiegeln der Festplatten (z.B. RAID)
- Getrennte Partitionen für Betriebssystem und Daten
- Notfallplan vorhanden (BSI-Standard 200-4)
- Regelmäßige Überprüfung des Notfallplans durch Test und Notfallübungen
- Gewährleistung der langfristigen technischen Lesbarkeit von Backupspeichermedien

3.2 Belastbarkeit (Widerstandsfähigkeit und Ausfallkontrolle)

Beschreibung: Soll Systeme befähigen, mit risikobedingten Veränderungen umgehen zu können und Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufzuweisen.

- Redundante Stromversorgung
- Redundante Datenanbindung
- Redundante Klimatisierung
- Ausweich-Rechenzentren vorhanden (Hot- bzw. Cold-Stand-by?): Hot
- sonstige redundante Systeme/Verfahren:
- Einsatz einer hochverfügbaren SAN-Lösung (Storage Area Network)
- Computer Emergency Response Team (CERT)
- Einsatz von Lastenverteilung (Load Balancing)
- Abgrenzung kritischer Komponenten
- Durchführung von Penetrationstests

- Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)
- Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates
- Regelmäßige Überprüfung der Konfiguration der Firewalls
- Regelmäßige Sensibilisierung der Mitarbeiter (mind. jährlich)
- Prozess zur unverzüglichen Meldung von Vorkommnissen an die IT ist allen Mitarbeitern bekannt
- Abschluss einer Cyber-Versicherung

4. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Kontrollverfahren

Beschreibung: Soll die Wirksamkeit der Datensicherheitsmaßnahmen gewährleisten.

- Verarbeitungsverzeichnisse (Art. 30 I und II DSGVO) werden jährlich aktualisiert
- Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
- Meldung neuer/veränderter Datenverarbeitungsverfahren an den IT-Sicherheitsbeauftragten
- Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert
- Regelmäßige Überprüfung und Auswertung der eingesetzten Software
- Konzepte und Dokumentationen werden regelmäßig geprüft (PDCA-Zyklus)
- Prüfung der Wirksamkeit getroffener Sicherheitsmaßnahmen mind. jährlich
- Durchführung von Sicherheitstests auf Webanwendungen nach Good-Practice-Vorgehen (z.B. OWASP Testing Guide)
- Bei Feststellungen im Rahmen der zuvor gen. Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst
- Prozess zur Reaktion auf Sicherheitsverletzungen (Angriffe) und Systemstörungen existiert (Incident-Response-Management)
- Dokumentation von Sicherheitsvorfällen
- Sicherheitszertifizierungen (ISO 27001, BSI IT-Grundschutz, ISIS12 etc.)
- Einsatz von Security Intelligence (Real Time-Analyse; log management, SIEMs, NBADs, network forensics)

4.2 Auftragskontrolle

Beschreibung: Soll sicherstellen, dass Daten, die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftraggebers verarbeitet werden.

- Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)
- Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)
- Vorabkontrollen beim Auftragnehmer vor Vertragsbeginn
- Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (Während Vertragsdauer)
- Vor-Ort-Kontrollen beim Auftragnehmer
- Überprüfung des Datensicherheitskonzepts beim Auftragnehmer

- Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer
- Auftragnehmer hat Datenschutzbeauftragten benannt

4.3 Trennungskontrolle

Beschreibung: Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt voneinander zu verarbeiten.

- Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)
- Physikalische Datentrennung (z.B. unterschiedliche Systeme oder Datenträger)
- Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)
- Datensicherungen der Auftraggeber-Daten auf separaten Datenträgern (ohne Daten anderer Kunden)
- Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt
- Trennung von Entwicklungs-, Test- und Produktivsystem
- Zuordnung von Datensätzen zu Zweckattributen
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei & Speicherung auf einem anderen System

4.4 Sonstiges Datenschutz- bzw. Sicherheitsmanagement

- Geeignete Organisationsstruktur für Informationssicherheit mit eindeutig festgelegten Rollen
- IT-Sicherheitsbeauftragter benannt
- Einsatz einer Datenschutzmanagement-Software
- Datenschutzbeauftragter benannt
- Dokumentierter Prozess zum Umgang mit IT-Sicherheitsvorfällen
- Dokumentierter Prozess zum Umgang mit Datenschutzvorfällen
- Klare Verantwortlichkeiten bei der Handhabung von Datenschutz- und Sicherheitsvorfällen
- Dokumentierter Prozess zur Sicherstellung von Betroffenenrechten
- zentrale, für alle Mitarbeiter zugängliche Ablage von Richtlinien/ Prozessen/ Verfahrensanweisungen
- Richtlinien/ Prozessen/ Verfahrensanweisungen sind im Unternehmen kommuniziert und allen Mitarbeitern bekannt
- Externe Dienstleister werden, soweit nötig, zur Verschwiegenheit verpflichtet
- Regelung zur wirksamen Datenlöschung auf Hardware, die vom Hersteller oder Dienstleister zurückgenommen werden
- Regelmäßige Schulungen zu den Richtlinien und Sicherheitsprozessen

Anlage 3

Subunternehmer

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1	**Name:**	Vimcar GmbH
	Anschrift:	Warschauer Str. 57, 10243 Berlin, Deutschland
	Kontakt:	datenschutz@vimcar.com
	Drittland:	Nein
	Zweck:	• Bereitstellung und Entwicklung der SaaS Vimcar Fahrtenbuch und Vimcar Fleet Geo • Kundensupport • Spedition
2.	**Name:**	Avrios International AG
	Anschrift:	Rieterstr. 6, 8002 Zürich, Schweiz
	Kontakt:	privacy@avrios.com
	Drittland:	Ja
	Garantie:	Angemessenheitsbeschluss der EU-Kommission, Art. 45 DSGVO
	Zweck:	• Bereitstellung der SaaS Avrios Flottenmanagement • Kundensupport