SERVICE-BEDINGUNGEN FÜR CONNECT FLEET

Teil 3: Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

Einführende Bestimmungen

Diese Anlage (Auftragsverarbeitungsvertrag) ist wesentlicher Bestandteil des Leasingvertrags und regelt, wie der Leasinggeber als Auftragsverarbeiter gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) personenbezogene Daten für den Dienst **Connect Fleet** im Auftrag des Leasingnehmers verarbeitet. Der Auftragsverarbeitungsvertrag verwendet in unveränderter Form die von der EU Kommission im Durchführungsbeschluss (EU) 2021/915 vom 4. Juni 2021 gemäß Art. 28 Abs. 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates veröffentlichten Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern für die Verarbeitung personenbezogener Daten innerhalb der Europäischen Union.

Der Leasingnehmer ist dafür verantwortlich, sicherzustellen, dass für die durch den Auftragsverarbeiter verarbeiteten personenbezogenen Daten eine gültige Rechtsgrundlage im Sinne der DSGVO vorliegt. Dies kann beispielsweise durch eine entsprechende Einwilligung der betroffenen Person oder eine anderweitige Rechtsgrundlage gemäß Art. 6 DSGVO gewährleistet werden.

Der Leasingnehmer stellt den Auftragsverarbeiter von sämtlichen Ansprüchen frei, die sich aus einer fehlenden Rechtsgrundlage für die Datenverarbeitung ergeben können.

Standardvertragsklauseln Auftragsverarbeitung

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln") soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 erfüllt werden.

Klausel 2
Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3
Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4
Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5
Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7

Pflichten der Parteien

7.1 Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4 Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6 Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 4 Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8 Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8
Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung"), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

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 den Artikeln 33 und 34 der Verordnung (EU) 2016/679 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls 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;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

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:

a) 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);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) 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.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III – SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 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.

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

   1) 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;

   2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 nicht erfüllt;

   3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 zum Gegenstand hat, nicht nachkommt.

c) 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.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I – LISTE DER PARTEIEN

A. Verantwortlicher:

Verantwortlicher ist der im Leasingantrag genannte Kunde.

B. Auftragsverarbeiter:

1. Auftragsverarbeiter ist:

Leasys S.p.A. Zweigstelle Deutschland
Friedrich-Lutzmann-Ring 1
65428 Rüsselsheim am Main
Deutschland

Telefon: 00 800 33442200
E-Mail: kontakt.de@leasys.com

2. Datenschutzbeauftragter beim Auftragsverarbeiter ist:

TRIADES Managementberatung
Herr Martin Lorenz
Am Hang 8, 31655 Stadthagen

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Gegenstand des Auftrags	Der Auftrag umfasst die Bereitstellung des Dienstes Free2Move Connect Fleet, der Leasingnehmern den Zugriff auf Fahrzeugnutzungsdaten mit folgenden Leistungsmerkmalen ermöglicht: • Verfolgung zurückgelegter Kilometer und Nutzungszeiten, tatsächlicher Kraftstoffverbrauch und -Füllstand, Echtzeit-Übermittlung mechanischer Warnmeldungen und Erinnerung an Wartungsintervalle • Fahrstilanalyse, personalisierte Empfehlungen für ökonomischeres Fahren, Fahrer-Ranking nach sicherer und effizienter Fahrweise

	• Geolokalisierung der Fahrzeuge in Echtzeit, Visualisierung gefahrener Routen, Geofencing und POI Manager
Dauer des Auftrags	Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des mit dem Kunden abgeschlossenen Leasingvertrags.
Art und Zweck der vorgesehenen Verarbeitung von Daten	Die Datenerfassung erfolgt über die in den Fahrzeugen eingebauten Telematik-Boxen. Die Verarbeitung der Daten findet auf Free2Move Connect Fleet Plattform statt und ist erforderlich, damit der Leasingnehmer als Verantwortlicher über die Plattform auf die Fahrzeugnutzungsdaten zugreifen kann. Die Datenverarbeitung erfolgt nach den Weisungen des Verantwortlichen (Fuhrparkmanagers) für folgende Zwecke der Fuhrparkverwaltung: Fleet Management: • Nutzung und Einsatzoptimierung einer Fahrzeugflotte, Eco-Driving-Analyse: • Reduzierung des Kraftstoffverbrauchs • Reduzieren von Verkehrsunfällen Eco-Charging: • Reduzierung des Stromverbrauchs • Identifizieren des optimalen Verbraucherverhaltens • Ermittlung des Rest-/Restwerts des Fahrzeugs
Kategorien betroffener Personen	Wir verarbeiten personenbezogene Daten der Mitarbeiter/Vertreter unserer Leasingnehmer im Rahmen der Bereitstellung von Fuhrparkmanagementdiensten.
Art der Daten	Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien: Daten der Vertreter des Leasingnehmers: • Name des Vertreters des Leasingnehmers • Position • E-Mail und Telefonnummer • Kontaktdaten inkl. Land und Sprache Vom Kunden/Benutzer generierte Daten: • Kennzeichen • Fahrzeug-Identifizierungsnummer (FIN) • Fahrzeugdaten (Marke, Kraftstoff, Klasse, Verkaufsdatum und Datum der Aktivierung des Fahrzeugs, Lieferdatum) • Zugehörige Fahrzeugflotte Fahrzeuggenerierte/-bezogene Daten: • Zündung und Motor Stopp • Kraftstoff- und Batterieladestand • Kilometerzähler • Kraftstoffverbrauch

	• Fahrzeug Warnungen • Fahrzeugpositionsdaten (GPS Breiten-/Längengrad, Fahrtrichtung, Höhe sowie Datum und Zeitstempel) Telematikeinheit generierte Daten / Fahrerverhaltensdaten: • Fahrerverhaltensdaten (Fahrzeuggeschwindigkeit, starkes Bremsen, abruptes Beschleunigen, übermäßiger Leerlauf, Nutzung des Sicherheitsgurts, Rückwärtsfahrten, Unfallerkennungen und zurückgelegte Kilometer pro Fahrt) • Datum und Uhrzeit der Aktivierung des Geräts Von der Plattform generierte Daten: • Fahrzeit • Fahrzeugwartungsmeldungen • Reiserouten und Fahrtenverlauf • Sitzungs- und Authentifizierungscookies
Sensible Daten gemäß Ziffer 7.5	Im Rahmen der Auftragsverarbeitung werden **keine** sensiblen Daten im Sinne von Ziffer 7.5 dieses Vertrags bzw. Art. 9 DSGVO verarbeitet.

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

I. Allgemein

Der folgende Abschnitt bietet einen Überblick über die technischen und organisatorischen Maßnahmen (TOMs), die von Leasys und seinen Unterauftragnehmern definiert und eingesetzt werden, um die in Artikel 32 DSGVO festgelegten Anforderungen umzusetzen. Dieses Dokument enthält die allgemeinen Maßnahmen, die umgesetzt und eingehalten werden, und gilt zusätzlich zu den spezifischen Sicherheitsmaßnahmen, die in mehreren separaten (IT-Sicherheits-)Richtlinien oder dokumentierten Verfahren/Prozessen beschrieben sind.

Darüber hinaus verweisen wir auch auf die IT-Sicherheitsstandards, die von AWS und Google Cloud implementiert wurden (unseren Haupt-Cloud-Anbietern) und bei denen wir fast alle (personenbezogenen) Daten speichern.

II. AWS

AWS hat folgende technische und organisatorische Maßnahmen für das AWS-Netzwerk umgesetzt und wird diese aufrechterhalten, wie in den AWS-Sicherheitsstandards und im AWS-GDPR DATA PROCESSING ADDENDUM beschrieben. Insbesondere hat AWS folgende technische und organisatorische Maßnahmen umgesetzt und wird diese aufrechterhalten:

- die Sicherheit des AWS-Netzwerks gemäß Abschnitt 1.1 der AWS-Sicherheitsstandards;
- die physische Sicherheit der Einrichtungen gemäß Abschnitt 1.2 der AWS-Sicherheitsstandards;

- Maßnahmen zur Kontrolle der Zugriffsrechte für AWS-Mitarbeiter und -Auftragnehmer in Bezug auf das AWS-Netzwerk gemäß Abschnitt 1.1 der AWS-Sicherheitsstandards; und
- Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der von AWS umgesetzten technischen und organisatorischen Maßnahmen, wie in Abschnitt 2 der AWS-Sicherheitsstandards beschrieben.

Die von AWS bereitgestellte IT-Infrastruktur wird in Übereinstimmung mit dem neuesten Stand der Technik und einer Vielzahl von IT-Sicherheitsstandards konzipiert und verwaltet. Im Folgenden finden Sie eine unvollständige Liste der Qualitätssicherungsprogramme, die AWS einhält:

- SOC 1/ISAE 3402, SOC 2, SOC 3
- FISMA, DIACAP und FedRAMP
- PCI DSS Level 1
- ISO 9001, ISO 27001, ISO 27017, ISO 27018

III. Google Cloud

Google Cloud hat die technischen und organisatorischen Maßnahmen für Google Workspace, wie in Abschnitt 7 der Vereinbarung zur Datenverarbeitung für Google Workspace und/oder ergänzende Produktvereinbarungen beschrieben, umgesetzt und wird diese aufrechterhalten. Insbesondere hat Google Cloud die folgenden technischen und organisatorischen Maßnahmen umgesetzt und wird diese aufrechterhalten:

- Sicherheitsmaßnahmen von Google gemäß Anhang 2 der Datenschutzvereinbarung von Google
- Zugang und Compliance
- Zusätzliche Sicherheitskontrollen
- Sicherheitsunterstützung von Google
- Datenvorfall-Management

Google wird für die geprüften Dienste mindestens Folgendes aufrechterhalten, um die anhaltende Wirksamkeit der Sicherheitsmaßnahmen zu bewerten:

- Zertifikate für ISO 27001, ISO 27017 und ISO 27018 (die „Compliance-Zertifizierungen"); und
- SOC 2- und SOC 3-Berichte, die vom externen Prüfer von Google erstellt und jährlich auf der Grundlage einer mindestens alle 12 Monate durchgeführten Prüfung aktualisiert werden (die „SOC-Berichte"). Google kann jederzeit Standards hinzufügen. Google kann eine Compliance-Zertifizierung oder einen SOC-Bericht durch eine gleichwertige oder verbesserte Alternative ersetzen.

IV. Leasys / Free2move

Im Folgenden finden Sie eine Übersicht über allgemeine TOMs:

1. **Grundlegende Sicherheitsmaßnahmen:**
   - Vorfallmanagement (incident management): Security Service Desk mit zentralem (Informations-) Sicherheitsvorfallprozess
   - Informationssicherheitsrichtlinie mit implementierten Sicherheitsgrundsätzen

2. **Informationssicherheitsmanagementsystem (ISMS):**
   - Zentrale Richtlinie für alle Mindest-IT-Sicherheitsmaßnahmen der Free2move SAS
   - Verbindlich für alle Tochtergesellschaften, IT-System-Betreiber und Nutzer
   - Definiert sicherheitsspezifische Anforderungen für alle Informations- und Telekommunikationstechnologien

   - **Hauptziele des ISMS:**
     - Gewährleistung der Vertraulichkeit und Integrität von Informationen
     - Sicherstellung der Verfügbarkeit geschäftsprozessunterstützender IT-Systeme
     - Schutz personenbezogener Daten gemäß geltendem Recht
     - Gewährleistung der Prüfbarkeit von IT-Systemen
     - Sicherstellung der Widerstandsfähigkeit gegen Angriffe

   - **Standardisierung und Grundprinzipien:**
     - Basiert auf ISO/IEC 27001:2013 & ISO/IEC 27002:2022
     - Organisierung der Informationssicherheit
     - Governance-Struktur für Informationssicherheitsrisiken
     - Regelungsrahmen für Informationssicherheitsprozesse
     - Überwachung und Bewertung von Überprüfungen

   - **Zentrale Aspekte:**
     - Zuverlässigkeit: Vertrauenswürdigkeit und Nachvollziehbarkeit von Informationen
     - Verantwortlichkeit: Zurechenbarkeit von Handlungen
     - Verbindlichkeit: Nachweisbarkeit von Ereignissen
     - Authentizität: Identitätsüberprüfung

3. **Darüber hinaus wurden folgende Maßnahmen umgesetzt (durch separate dokumentierte Richtlinien/Prozesse geregelt):**
   - Segregation of Duties
   - Kontakt mit Behörden und Interessengruppen
   - Teleworking Policy (draft, not active yet)
   - Terms and Conditions of Employment (HR Security)

- Information Security Awareness, Education and Training
- Termination or Change of Employment Responsibilities (HR Security)
- Acceptable Use of Assets
- Return of Assets Policy
- Secure Coding (draft, not active yet)
- Liability Agreements between Free2move and Business Partners for the Usage of Free2move API
- Management of Technical Vulnerabilities (work in progress)
- Guidelines for Vulnerability Management exist (draft, not active yet)
- Risk Management (draft, not active yet)
- Risk Assessments (draft, not active yet)
- Risk Treatment Plans (draft, not active yet)
- Security in Development and Support Processes (draft, not active yet)
- Data Classification Policy (draft, not active yet)
- Information Security Incident Management
- Defined Responsibilities and Procedures

4. Vertraulichkeit, Pseudonymisierung und Verschlüsselung, Art. 32 DSGVO

- **Technische Maßnahmen:**
  - Regelmäßige System- und Software-Updates
  - Regelmäßige Schwachstellenprüfungen aller Systeme
  - Verschlüsselung von Informationssystemen als Standard
    - Cryptography
    - Configuration templates through Infrastructure as Code
  - Passwort-Management: 1 Password
  - Netzwerksegmentierung: AWS Multi-Account Strategy/Architecture
  - SSL-Zertifikate für Websites (https: //)
  - Firewalls:
    - AWS Network ACLs
    - AWS Security Groups
  - Web Application Firewall: Nginx mit Modsecurity und OWASP Core Rule Set
  - ACL limitation for external access administration: Inbound rules limitation for EC2
  - Schwachstellen-Scanning (Vulnerability Management Process) mit Snyk (work in progress) & GitLab Dependency Scanner (work in progress)
  - Identity and Access Management
    - Currently AWS IAM but Okta in the future (work in progress)
      - User Access Provisioning
      - Management of Privileged Access Rights
      - Use of Secret Authentication Information
      - Secure Log-on Procedures

        - Role-Based Access Control (RBAC)
      - Multi-Factor Authentication: SMS, Google Authenticator
    - Getrennte Umgebungen für Production und Non-Production Systeme
    - Free2move API Guidelines:
      - Authentication und Authorization durch SAML und mTLS
      - No read-access für Kundendaten
    - Automatisierung in Bezug auf Kundendaten und Einwilligungen / Lebenszyklus von Kundendaten
      - Automatisierte Datenbereinigung nach 3 Jahren Inaktivität
      - Automatisierte Löschung von Nutzerdaten
      - Automatisiertes Herunterladen von Benutzerdaten für authentifizierte und validierte Benutzer
      - Individuelle Aufbewahrungs-/Löschkonzepte je nach Zweck der Datenerhebung
- **Organisatorische Maßnahmen**
    - Verwaltung und Überprüfung von privilegierten Zugriffsrechten (interne Tools für unser Backoffice und CloudTracker für AWS)
      - Zugriffsanfragen für Assets mit hoher Priorität werden zusätzlich durch Einzelgespräche überprüft und validiert
    - Richtlinie zur Zugriffskontrolle
    - Richtlinie für den Zugriff auf Netzwerke und Netzwerkdienste
    - Benutzerregistrierung und -abmeldung (Benutzerverwaltung)
    - Regelmäßige Überprüfung der Benutzerzugriffsrechte (vierteljährlich)
    - Richtlinie/Maßnahmen für physische Zugangskontrollen
      - Türmanagementsystem Unifi Protect
    - Der Zugriff auf personenbezogene Daten ist auf eine begrenzte Gruppe von Mitarbeitern beschränkt, die sich mit ihrem zugewiesenen Login anmelden müssen
    - Anmeldeinformationen (Benutzer-ID und Passwort) und Zugriff erfolgen ausschließlich über verschlüsselte Mittel (HTTPS, TLS/SSL).
    - Gruppenkonten/Systemanmeldungen nur für bestimmte Anwendungen.
    - Benutzer-IDs werden sofort deaktiviert/gelöscht, wenn Mitarbeiter das Unternehmen verlassen.
    - Passwörter werden nicht im Klartext gespeichert oder unverschlüsselt übertragen.
    - Wo immer möglich, wird eine Zwei-Faktor-Authentifizierung verwendet.
    - Sitzungsverwaltung.
    - Getrennte Umgebungen für Produktions- und Nicht-Produktionssysteme
    - Verwendung von Geheimhaltungsvereinbarungen (NDAs)
    - Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
    - Einhaltung und Berücksichtigung von Datenschutzgrundsätzen wie Datenminimierung, Datenschutz durch Technikgestaltung und datenschutzfreundliche
    - Standard in Bezug auf den Umfang der Datenverarbeitung, die Menge der erhobenen personenbezogenen Daten und die Aufbewahrungs- und Löschfristen

5. Integrität, Art. 32 (1) lit. b GDPR

- **Technische Maßnahmen:**
  - Cloud Security Posture Management: CloudMapper & Prowler mit CIS AWS Foundations Benchmark-Standard
  - Webanwendung Nginx mit Modsecurity und OWASP Core Rule Set
  - Vulnerability Scanning (Vulnerability Management Process) mit Snyk (in Arbeit) & GitLab Dependency Scanner (in Arbeit)
  - Getrennte Umgebungen für Produktions- und Nicht-Produktionssysteme
  - Security Logging Concept
    - Basic Logging auf allen Systemen
    - Detaillierte Protokollierung für alle privilegierten Aktivitäten
    - Zentralisierte Protokollspeicherung in AWS OpenSearch, Cloudtrail & CloudWatch
  - CI/CD-Pipeline: Kubernetes (in Arbeit)
    - 4-Augen-Prinzip durch Pull-/Merge-Anfragen
    - Alle Änderungen müssen die Pipeline durchlaufen
    - Automatisierte Sicherheitstests bei jedem Build
  - Containersicherheit:
    - Sicherheits-Baseline: Terraform
  - Sicherheit mobiler Anwendungen:
    - Binärdateien werden mit den bereitgestellten Zertifikaten der offiziellen App-Stores signiert
  - Free2move-API-Richtlinie:
    - Eingabevalidierung und Plausibilitätsprüfungen
    - Stichproben
  - Kundendaten:
    - Bruteforce-Schutzmechanismen und interne Honeypot-Lösung
    - IP-Reputations-Zugriffsüberwachung

- **Organisatorische Maßnahmen**
  - Richtlinie zur Zugriffskontrolle
  - Zugriff auf Netzwerke und Netzwerkdienste
  - Benutzerregistrierung und -abmeldung
  - Regelmäßige Überprüfung der Benutzerzugriffsrechte
  - Richtlinie zum Änderungsmanagement

6. Verfügbarkeit und Belastbarkeit, Art. 32 (1) lit. b und c DSGVO

- **Technische Maßnahmen:**
  - AWS Content Delivery Network (CDN): AWS CloudFront
  - Webanwendung Nginx mit Modsecurity und OWASP Core Rule Set
  - Vulnerability Scanning (Vulnerability Management Process) mit Snyk (in Arbeit) & GitLab Dependency Scanner (in Arbeit)
  - Getrennte Umgebungen für Produktions- und Nicht-Produktionssysteme
  - Redundanz: AWS Availability Zones
  - Automatisierte Backups aller Systeme

- **Organisatorische Maßnahmen**
  - Verfügbarkeitskontrolle: Schutz vor versehentlicher Beschädigung, Zerstörung oder Verlust: hochverfügbare Speicherdienste, Aufbewahrungssperren, Eskalationswege und Notfallpläne
  - Datenverarbeitung: Keine Datenverarbeitung gemäß Art. 28 DSGVO ohne entsprechende Anweisungen des Datenverantwortlichen, formalisiertes Management und strenge Auswahl der Dienstleister, Nachkontrollen
  - Ausfallsicherheit: Systeme und Dienste (z. B. Speicher, Zugriff, Leitungskapazitäten usw.) sind so konzipiert, dass auch zeitweise hohe Belastungen oder hohe konstante Verarbeitungslasten gewährleistet werden können
  - Unterstützende Dienstprogramme
  - Physische Sicherheitszone: Wartung der Ausrüstung

7. Verfahren zur regelmäßigen Überprüfung und Bewertung, Art. 32 (1) lit. d DSGVO

- Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen auf Wirksamkeit und Plausibilität und allgemeine Prozesse zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten
- Wiederholte Anpassung des umgesetzten allgemeinen Datenschutz-/Datenschutzmanagements und der Maßnahmen einschließlich Berichterstattung
- Wiederholte Anpassung des Vorfallsreaktionsmanagements
- Regelmäßige Bewertung, IT-Audits, Verfolgung von (ISO-)Zertifizierungen

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche genehmigt die Inanspruchnahme folgender Unterauftragsverarbeiter:

Eingesetzte Unterauftragsverarbeiter

#	Firma	Ort	Erbrachte Leistung
1	Free2Move SAS 45 rue de la Chaussée d'Antin 75009, PARIS , ILE-DE-RANCE France	Frankreich	Bereitstellung der Plattform
2	Amazon Web Services EMEA Sarl	Europa	IT-Dienstleister für: Server-Hosting, Cloud-Computing, Datenspeicherung, Datenbankverwaltung
3	Google Cloud Services	Europa	IT-Dienstleister für: Server-Hosting, Cloud-Computing, Datenspeicherung, Datenbankverwaltung
4	PSA Automobiles SA	Europa, Frankreich	Übermittlung personenbezogener Daten an die jeweiligen IT-Dienstleister zur Unterstützung der genannten Zwecke
5	FCA Italy S.p.A, Corso Agnelli 200, 10135 Torino	Europa, Italien	Übermittlung personenbezogener Daten an die jeweiligen IT-Dienstleister zur Unterstützung der genannten Zwecke
6	MongoDB Limited	Europa	Datenbank
7	Kuantic M2M & Telematics	Europa	Hardware und Telematic Service Provider