

AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV) FÜR VDO FLEET SERVICES (ANNEX C)

Dieser AVV regelt die gesetzlichen Verpflichtungen der PARTEIEN in Bezug auf den Datenschutz, die sich aus der Verarbeitung personenbezogener Daten im Zusammenhang mit dem jeweiligen Vertrag über VDO FLEET SERVICES mit dem Kunden ergeben. Die folgenden AVV basieren auf den offiziellen Standardvertragsbedingungen, die von der EU-Kommission im Durchführungsbeschluss (EU) 2021/915 der Kommission festgelegt wurden.

Der Kunde als "Verantwortlicher" und die CONTINENTAL AUTOMOTIVE TECHNOLOGIES GMBH als "Auftragsverarbeiter" vereinbares Folgendes:

ABSCHNITT 1

1. ZWECK UND ANWENDUNGSBEREICH

- 1.1 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 (Datenschutz-Grundverordnung).
- 1.2 Der oben aufgeführte Verantwortliche und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.
- 1.3 Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anlage 1.
- 1.4 Die Anlagen 1 bis 3 sind Bestandteil der Klauseln.
- 1.5 Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.
- 1.6 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 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

2. UNABÄNDERBARKEIT DER KLAUSELN

- 2.1 Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anlagen angegebenen Informationen.
- 2.2 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.

3. AUSLEGUNG

- 3.1 Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
- 3.2 Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.
- 3.3 Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

4. VORRANG / RANGFOLGE

- 4.1 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.

5. KOPPELUNGSVERBOT

- 5.1 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 Anlagen ausfüllt und diese AVV unterzeichnet.
- 5.2 Nach Ausfüllen und Unterzeichnen der unter 5.1 genannten Anlagen wird die beitretende Einrichtung als Partei dieser Klauseln

VDO FLEET ONLINE

- ANNEX C "AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV) FÜR VDO FLEET SERVICES" - (CONTINENTAL AFTERMARKET & SERVICES GMBH, VERSION 1.6, 04.07.2024)

behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Mitunterzeichnung des AVV.

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

ABSCHNITT II

6. BESCHREIBUNG DER VERARBEITUNG

- 6.1 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 Anlage 1 aufgeführt.

7. PFLICHTEN DER PARTEIEN

7.1 Weisungen

- 7.1.1 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.

- 7.1.2 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

- 7.2.1 Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anlage 1 genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3 Dauer der Verarbeitung personenbezogener Daten

- 7.3.1 Die Daten werden vom Auftragsverarbeiter nur für die in Anlage 1 angegebene Dauer verarbeitet.

7.4 Sicherheit der Verarbeitung

- 7.4.1 Der Auftragsverarbeiter ergreift mindestens die in Anlage 2 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.

- 7.4.2 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

- 7.5.1 Falls die Verarbeitung personenbezogener 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

- 7.6.1 Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
- 7.6.2 Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
- 7.6.3 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 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die

VDO FLEET ONLINE

- ANNEX C "AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV) FÜR VDO FLEET SERVICES" - (CONTINENTAL AFTERMARKET & SERVICES GMBH, VERSION 1.6, 04.07.2024)

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.

- 7.6.4 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.
- 7.6.5 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

- 7.7.1 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 dreißig (30) Tage 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. Erhebt der für die Verarbeitung Verantwortliche nicht innerhalb von dreißig (30) Tagen Einspruch, so gilt seine Zustimmung als erteilt.

Der Verantwortliche erklärt sich hiermit mit der Einbeziehung der in Anlage 3 aufgelisteten Unterauftragsverarbeiter einverstanden.

- 7.7.2 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 und/oder der Verordnung (EU) 2018/1725 unterliegt.
- 7.7.3 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.
- 7.7.4 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.

7.8 Internationale Datenübermittlungen

- 7.8.1 Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt – unbeschadet der Bestimmung unter Punkt 7.8.2 – ausschließlich
- 7.8.1.1 auf der Grundlage dokumentierter Weisungen des Verantwortlichen,
- 7.8.1.2 auf der Grundlage einer vorherigen (allgemeinen) Zustimmung des Verantwortlichen, oder
- 7.8.1.3 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 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

- 7.8.2 Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Punkt 7.7 mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) und beinhalten diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679, stimmt der Verantwortliche zu, dass eine solche Verarbeitung zulässig ist, sofern

7.8.2.1 die Verarbeitung in einem Land durchgeführt wird, für das die EU-Kommission einen entsprechenden Angemessenheitsbeschluss auf der Grundlage von Artikel 45 der Verordnung (EU) 2016/679 erlassen hat, oder

7.8.2.2 der Auftragsverarbeiter und Subauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 angenommen wurden.

7.8.3 Der Verantwortliche stimmt hiermit der Übermittlung und Verarbeitung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 durch die in Anlage 3 angeführten Auftragsverarbeiter und/oder Unterauftragsverarbeiter zu.

8. UNTERSTÜTZUNG DES VERANTWORTLICHEN

- 8.1 Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person

VDO FLEET ONLINE

- ANNEX C "AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV) FÜR VDO FLEET SERVICES" - (CONTINENTAL AFTERMARKET & SERVICES GMBH, VERSION 1.6, 04.07.2024)

erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

- 8.2 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 Punkten 8.1 und 8.2 befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.
- 8.3 Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Punkt 8.2 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:
 - 8.3.1 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;
 - 8.3.2 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;
 - 8.3.3 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;
 - 8.3.4 Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.
- 8.4 Die Parteien legen in Anlage 2 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.

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 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 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:

- 9.1.1 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);
 - 9.1.2 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:
 - 9.1.2.1 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;
 - 9.1.2.2 die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - 9.1.2.3 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;
- 9.1.3 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:

- 9.2.1 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);
- 9.2.2 Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
- 9.2.3 die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des

VDO FLEET ONLINE

- ANNEX C "AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV) FÜR VDO FLEET SERVICES" - (CONTINENTAL AFTERMARKET & SERVICES GMBH, VERSION 1.6, 04.07.2024)

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 Anlage 2 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

10. VERSTÖSSE GEGEN DIE KLAUSELN UND BEENDIGUNG DES VERTRAGS

- 10.1 Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – 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.
- 10.2 Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
- 10.2.1 der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Punkt 10.1 ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
- 10.2.2 der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;
- 10.2.3 der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.
- 10.3 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 Punkt 7.1.2 verstoßen.
- 10.4 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.

11. ÜBERSICHT DER ANLAGEN

- Anlage 1: Details zur Verarbeitung
- Anlage 2: Technische und organisatorische Maßnahmen
- Anlage 3: Unterauftragsverarbeiter

ANLAGE 1- DETAILS ZUR VERARBEITUNG

1. GEGENSTAND DER BEAUFTRAGUNG:

CONTINENTAL ist beauftragt, als Auftragsverarbeiter tätig zu werden, um im Auftrag des KUNDEN (des Verantwortlichen) die personenbezogenen Daten zu verarbeiten, die zur Erbringung der Leistungen der VDO FLEET-Anwendung erforderlich sind.

2. ART UND ZWECK DER DATENVERARBEITUNG:

- 2.1 CONTINENTAL ist berechtigt, personenbezogene Daten nur nach Maßgabe des VDO FLEET Services VERTRAGES und der Weisungen des KUNDEN zu erheben, zu verarbeiten und zu nutzen (siehe Ziffer 9).
- 2.2 Einzelheiten zu Umfang, Art und Zweck der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten ergeben sich aus den Allgemeinen Geschäftsbedingungen des Hauptvertrages, seiner Leistungsbeschreibung sowie den Funktionsübersichten der Produkte.

3. KATEGORIEN VON BETROFFENEN PERSONEN:

- | | |
|--|---|
| <input checked="" type="checkbox"/> KUNDEN | <input type="checkbox"/> Besucher |
| <input type="checkbox"/> Veranstaltungsteilnehmer | <input checked="" type="checkbox"/> Benutzer der Services |
| <input checked="" type="checkbox"/> Kommunikationsteilnehmer | <input checked="" type="checkbox"/> Abonnenten |
| <input type="checkbox"/> Interessenten | |

VDO FLEET ONLINE

- ANNEX C "AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV) FÜR VDO FLEET SERVICES" - (CONTINENTAL AFTERMARKET & SERVICES GMBH, VERSION 1.6, 04.07.2024)

- | | |
|---|---|
| <input type="checkbox"/> Lieferant und/oder Dienstleister (individuelle Kontakte bei diesen Anbietern) | |
| <input checked="" type="checkbox"/> Arbeitnehmer | <input type="checkbox"/> Bewerber |
| <input type="checkbox"/> Ehemalige Arbeitnehmer | <input type="checkbox"/> Auszubildende/Praktikanten |
| <input type="checkbox"/> Angehörige von Arbeitnehmern | <input type="checkbox"/> Berater |
| <input checked="" type="checkbox"/> Handelsvertreter/Vertriebsmitarbeiter | <input type="checkbox"/> Aktionäre / Organe |
| <input checked="" type="checkbox"/> Geschäftliche Ansprechpartner | <input type="checkbox"/> Zulieferer und Dienstleister |
| <input checked="" type="checkbox"/> Geschäftspartner | |
| <input checked="" type="checkbox"/> Sonstige, bitte angeben: Arbeitnehmer von Kunden, d.h. Fahrer und Anwender von VDO FLEET-SERVICES | |

4. KATEGORIEN VON PERSONENBEZOGENEN DATEN

Allgemeine Daten/Private Kontaktinformationen

- | | |
|--|--|
| <input checked="" type="checkbox"/> Name(n), persönliches Profil | <input type="checkbox"/> Foto |
| <input checked="" type="checkbox"/> Private Anschrift | <input checked="" type="checkbox"/> Geburtsdatum |
| <input checked="" type="checkbox"/> Identifikationskartendaten (z.B. Pass, Sozialversicherungsnummer, Fahrerlaubnis) | |
| <input type="checkbox"/> Sonstige, bitte angeben: _____ | |

Vertragsdaten

- | | |
|---|--|
| <input checked="" type="checkbox"/> Abrechnungs- und Zahlungsdaten | <input checked="" type="checkbox"/> Bankverbindung/Kreditkartendaten |
| <input checked="" type="checkbox"/> Finanzielle Situation/ Kreditwürdigkeit | <input checked="" type="checkbox"/> Vertragshistorien |
| <input type="checkbox"/> Sonstige, bitte angeben: _____ | |

Berufliche Daten

- | | |
|--|---|
| <input checked="" type="checkbox"/> Persönliche Angaben | <input type="checkbox"/> Angaben zu Position und Beschäftigungsverhältnis |
| <input checked="" type="checkbox"/> Leistungsmanagement | <input type="checkbox"/> Angaben zu Qualifikation und Ausbildung |
| <input checked="" type="checkbox"/> Sozialversicherungsangaben | <input checked="" type="checkbox"/> Abwesenheit von der Arbeit |
| <input checked="" type="checkbox"/> Sonstige, bitte angeben: | |
| <ul style="list-style-type: none">• Zulassungsdaten des Kunden und seiner Fahrer/Nutzer• Fahrerdaten (z. B. Name, Adresse (Firmenadresse oder Privatadresse, soweit einschlägig), Geschlecht, Geburtsdatum, Lizenz- oder Führerscheinnummer, Fahrerkarte etc.)• Fahrzeugdaten und Fahrzeugprofile• Kommunikationsdaten (z.B. Telefon, E-Mail)• Bewegungsdaten, GPS-Daten• Tätigkeiten der Fahrer und Einsatzprofile, einschließlich Lenk- und Ruhezeiten gemäß Anlage 1B der Verordnung (EU) Nr. 561/2006, Verordnung (EU) Nr. 2020/1054, Verordnung (EG) Nr. 1360/2002, Verordnung Nr. 165/2014 und Durchführungsverordnung (EU) Nr. 2016/799• Daten für die Nutzung des Dienstes durch die Nutzer• Download-Daten für die Fahrerkarte und den Fahrtenschreiber. | |

Service- und IT-Nutzungsdaten

- | | |
|---|--|
| <input type="checkbox"/> Gerätekennungen | <input checked="" type="checkbox"/> Nutzungs- und Verbindungsdaten |
| <input type="checkbox"/> Bild-/Videodaten | <input checked="" type="checkbox"/> Telekommunikationsdaten/Mitteilungsinhalte |
| <input type="checkbox"/> Audio-/ Sprachdaten | <input type="checkbox"/> Identifikationsdaten |
| <input checked="" type="checkbox"/> Zugangsdaten | <input type="checkbox"/> Autorisierung/Zulassungen |
| <input type="checkbox"/> Metadaten | |
| <input type="checkbox"/> Sonstige, bitte angeben: _____ | |

Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen

Besondere Kategorien von personenbezogenen Daten

- | | |
|--|--|
| <input type="checkbox"/> Nationalität | <input type="checkbox"/> Religiöse oder weltanschauliche Überzeugungen |
| <input type="checkbox"/> Physische oder mentale Gesundheit | <input type="checkbox"/> Politische Meinungen |
| <input type="checkbox"/> Biometrische Daten | <input type="checkbox"/> Genetische Daten |
| <input type="checkbox"/> Gewerkschaftszugehörigkeit | <input type="checkbox"/> Sexuelle Orientierung |
| <input type="checkbox"/> Strafraten, Verurteilungen oder Urteile | |
| <input type="checkbox"/> Sonstige, bitte angeben: _____ | |

5. DAUER DER VERARBEITUNG

- 5.1 Die Dauer der Verarbeitung richtet sich nach der Laufzeit des (Haupt-)Vertrags und/oder etwaiger Einzelverträge oder Aufträge auf der Grundlage einer Rahmenvereinbarung.
- 5.2 Bis zur Beendigung der Verarbeitung und vorbehaltlich anderer dokumentierter Anweisungen des Verantwortlichen gibt der Auftragsverarbeiter dem Verantwortlichen oder einem vom Verantwortlichen benannten Dritten alle in seinem Besitz gelangten Unterlagen, Datenträger, Verarbeitungsergebnisse und Daten zurück, die im Zusammenhang mit dem Vertragsverhältnis verarbeitet wurden oder im Rahmen der Ausführung des Vertrags und/oder der Richtlinie (EU) 2016/679 entstanden sind.
- Diese Verpflichtung erstreckt sich auf Kopien und/oder Vervielfältigungen von Datenträgern und/oder Datenbeständen. Ein Zurückbehaltungsrecht in Bezug auf die genannten Daten und Datenträger besteht nicht. Sofern der Vertrag nichts anderes vorsieht, gibt der Auftragsverarbeiter dem Verantwortlichen alle Daten und Datenträger unentgeltlich zurück. Der Auftragsverarbeiter trägt alle Kosten und sonstige Ausgaben im Zusammenhang mit der Rückgabe der Daten.
- 5.3 Der Verantwortliche kann die Löschung der beim Auftragsverarbeiter gespeicherten Daten nicht verlangen, wenn der

VDO FLEET ONLINE

**- ANNEX C "AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV) FÜR VDO FLEET SERVICES" -
(CONTINENTAL AFTERMARKET & SERVICES GMBH, VERSION 1.6, 04.07.2024)**

Auftragsverarbeiter gesetzlich zur Aufbewahrung verpflichtet ist. Anstelle der Löschung kann die Datenverarbeitung eingeschränkt werden, soweit dies datenschutzrechtlich zulässig und möglich ist. Dies gilt insbesondere dann, wenn die Löschung aufgrund der spezifischen Speichermethoden nicht oder nur mit unverhältnismäßig hohem Aufwand verbunden ist.

ANLAGE 2 - TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Die Corporate Policy Continental Information Security Guideline (CISG) definiert die **Mindestanforderungen** an technische und organisatorische Maßnahmen bei CONTINENTAL im Umgang mit Informationen. Je nach Klassifizierung der Informationen sind Maßnahmen implementiert, die über die Mindestanforderungen hinausgehen.

Die Anforderungen der CISG werden im Unternehmen auf Basis des Corporate Standard Information Security Framework und des dazugehörigen Information Security Management Systems (ISMS) umgesetzt.

- Corporate Policy Continental Information Security Guideline (CISG)
- Corporate Standard Information Security Framework
- Annex 1 - Information Security Management System (ISMS)
- Annex 2 - Roles & Responsibilities in Information Security - RACI Chart

1. ZUTRITTSKONTROLLE

Sicherung des physischen Zutritts / Zugangs zu Verarbeitungssystemen, mit denen die Verarbeitung erfolgt, gegen Unbefugte (z.B. durch physischen Objektschutz: Zaun, Sicherheitspersonal, Türschlösser, Drehkreuz, Tür mit Kartenleser, Kameraüberwachung, organisatorischer Objektschutz, Zutrittsberechtigung, Zutrittsregistrierung).

- Corporate Standard Classification of Security Zones
- Annex 1 - Layout and Security Requirements
- Annex 2 - Audio/Visual Recording in Locations
- Corporate Standard Continental ID Cards

Spezifizierungen zu den Maßnahmen:

<input checked="" type="checkbox"/>	Alarmanlage
<input checked="" type="checkbox"/>	Automatisches Zutrittskontrollsystem
<input type="checkbox"/>	Schließanlage mit Codesperre
<input type="checkbox"/>	Biometrische Zutrittssperren
<input type="checkbox"/>	Lichtschranken/Bewegungsmelder
<input checked="" type="checkbox"/>	Manuelle Schließanlage inkl. Schlüsselregelung (Schlüsselbuch, Schlüsselausgabe)
<input checked="" type="checkbox"/>	Besucherprotokollierung
<input checked="" type="checkbox"/>	Sorgfältige Auswahl des Sicherheitspersonals
<input checked="" type="checkbox"/>	Chipkarten/Transponder-Schließsysteme
<input checked="" type="checkbox"/>	Videoüberwachung der Zugangstüren
<input checked="" type="checkbox"/>	Sicherheitsschlösser
<input checked="" type="checkbox"/>	Personenkontrolle durch Pförtner/Rezeption
<input checked="" type="checkbox"/>	Sorgfältige Auswahl des Reinigungspersonals
<input checked="" type="checkbox"/>	Tragepflicht von Mitarbeiter-/Gästeausweisen
<input type="checkbox"/>	Sonstiges:

2. ZUGANGSKONTROLLE/BENUTZERKONTROLLE

Verhinderung der Nutzung von automatisierten Verarbeitungssystemen durch Unbefugte mittels Datenübertragungseinrichtungen (z. B. Bildschirmschoner mit Passwörtern).

- Corporate Manual Password Regulation (M60.02.01)
- Corporate Standard Procedure for Identification and Authorization of Users of IT Systems
- Corporate Standard CUSTOMER Security Regulation (ersetzt M60.02.10)
- Corporate Standard Mobile Environment Governance (ersetzt M60.05.01)

VDO FLEET ONLINE

**- ANNEX C "AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV) FÜR VDO FLEET SERVICES" -
(CONTINENTAL AFTERMARKET & SERVICES GMBH, VERSION 1.6, 04.07.2024)**

Spezifizierungen zu den Maßnahmen:

<input checked="" type="checkbox"/>	Authentifizierung mit Benutzername/Passwort (Passwortvergabe erfolgt auf Basis der gültigen Passwortvorschriften)
<input type="checkbox"/>	Einsatz von Einbrucherkennungssystem
<input checked="" type="checkbox"/>	Einsatz von Anti-Viren-Software
<input checked="" type="checkbox"/>	Einsatz einer Firewall-Software
<input checked="" type="checkbox"/>	Anlegen von Benutzerprofilen
<input checked="" type="checkbox"/>	Zuordnung von Benutzerprofilen zu IT-Systemen
<input checked="" type="checkbox"/>	Einsatz von VPN-Technologie
<input checked="" type="checkbox"/>	Verschlüsselung von mobilen Datenträgern
<input type="checkbox"/>	Verschlüsselung von Datenträgern in Laptops
<input type="checkbox"/>	Einsatz einer zentralen Smartphone-Administrations-Software (z. B. zur externen Datenlöschung)
<input type="checkbox"/>	Sonstiges:

3. DATENZUGRIFFSKONTROLLE / DATENTRÄGERKONTROLLE / SPEICHERKONTROLLE

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle), Verhinderung der unbefugten Eingabe personenbezogener Daten sowie der unbefugten Kenntnisnahme, Modifizierung und Löschung gespeicherter personenbezogener Daten (Speicherkontrolle).

Sicherstellung, dass die zur Nutzung eines automatisierten Verarbeitungssystems berechtigten Personen nur aufgrund ihrer Zugriffsberechtigung Zugriff auf die personenbezogenen Daten haben (z.B. durch Berechtigungskonzepte, Passwörter, Austritts- und Versetzungsregelungen von Mitarbeitern) (Datenzugriffskontrolle).

Corporate Manual Password Regulation (M60.02.01)
Corporate Standard Procedure for Identification and Authorization of Users of IT Systems
Corporate Standard Classification and Control of Information
Corporate Manual Security Guidelines for Databases - 3.4.6 Data Integrity

Spezifizierungen zu den Maßnahmen:

<input checked="" type="checkbox"/>	Rollen und Berechtigungen auf Basis eines „Need to Know Prinzips“
<input checked="" type="checkbox"/>	Anzahl der Administratoren auf das „Nötigste“ reduziert
<input checked="" type="checkbox"/>	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
<input checked="" type="checkbox"/>	Physische Löschung von Datenträgern vor Wiederverwendung
<input checked="" type="checkbox"/>	Einsatz von Aktenvernichtern oder Dienstleistern
<input checked="" type="checkbox"/>	Verwaltung der Rechte durch definierte Systemadministratoren
<input checked="" type="checkbox"/>	Passwortrichtlinien inkl. Passwortlänge und Passwortwechsel
<input checked="" type="checkbox"/>	Sichere Aufbewahrung von Datenträgern
<input checked="" type="checkbox"/>	Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
<input type="checkbox"/>	Protokollierung der Vernichtung
<input type="checkbox"/>	Sonstige:

4. WEITERGABEKONTROLLE / TRANSPORTKONTROLLE

Sicherstellung der Vertraulichkeit und Integrität von Daten bei der Übermittlung personenbezogener Informationen und beim Transport von Datenträgern (z. B. durch leistungsfähige Verschlüsselung von Datenübertragungen, geschlossene Umschläge bei Mailings, verschlüsselte Speicherung auf Datenträgern).

Corporate Standard Classification and Control of Information

Spezifizierungen zu den Maßnahmen:

<input checked="" type="checkbox"/>	Einrichtungen von Standleitungen oder VPN-Tunneln
<input checked="" type="checkbox"/>	Verschlüsselte Datenübertragung im Internet (z.B. HTTPS, SFTP, etc.)
<input checked="" type="checkbox"/>	E-Mail-Verschlüsselung (Transportverschlüsselung)
<input checked="" type="checkbox"/>	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarten Löschfristen
<input type="checkbox"/>	Beim physischen Transport: Sorgfältige Auswahl von Transportpersonal und -fahrzeugen
<input type="checkbox"/>	Übermittlung von Daten in anonymisierter oder pseudonymisierter Form
<input type="checkbox"/>	Beim physischen Transport: Sichere Transportbehälter / -verpackungen
<input type="checkbox"/>	Sonstige:

5. EINGABEKONTROLLE/ÜBERMITTLUNGSKONTROLLE

Sicherstellung der nachträglichen Protokollierung und Überprüfung von Änderungen (welche personenbezogenen Daten wurden wann und von wem eingegeben oder verändert) innerhalb automatisierter Verarbeitungssysteme (Eingabekontrolle). Sicherstellung der ausreichend gesicherten und dokumentierten Übermittlung (einschließlich der verwendeten sicheren und angemessenen Übermittlungsmethoden) personenbezogener Daten je nach geografischer, physischer oder elektronischer Übermittlung an andere Orte (Übermittlungskontrolle).

Continental Information Security Guideline (CISG) – 3.5.10.1 Audit Logging
Corporate Standard Procedure for Identification and Authorization of Users of IT Systems
Corporate Standard Classification and Control of Information
Corporate Manual Security Guidelines for Databases - 3.4.6 Data Integrity

VDO FLEET ONLINE

**- ANNEX C "AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV) FÜR VDO FLEET SERVICES" -
(CONTINENTAL AFTERMARKET & SERVICES GMBH, VERSION 1.6, 04.07.2024)**

Spezifizierungen zu den Maßnahmen:

<input checked="" type="checkbox"/>	Protokollierung der Eingabe, Änderung und Löschung von Daten
<input checked="" type="checkbox"/>	Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch eindeutige Benutzernamen (nicht Benutzergruppen)
<input checked="" type="checkbox"/>	Vergabe von Rechten für die Erfassung, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
<input type="checkbox"/>	Erstellung einer Übersicht, welche Daten mit welchen Anwendungen erfasst, geändert und gelöscht werden können
<input type="checkbox"/>	Aufbewahrung von Formularen, aus denen Daten in die automatisierte Verarbeitung übernommen werden
<input type="checkbox"/>	Sonstige:

6. VERFÜGBARKEITSKONTROLLE / WIEDERHERSTELLUNG / ZUVERLÄSSIGKEIT / DATENINTEGRITÄT

Sicherstellung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können (Wiederherstellbarkeit). Sicherstellung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Funktionsstörungen gemeldet werden (Zuverlässigkeit). Sicherstellung, dass gespeicherte personenbezogene Daten nicht durch Funktionsstörungen des Systems beschädigt werden können (Datenintegrität). Sicherstellung, dass personenbezogene Daten vor versehentlicher Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle), z.B. durch Implementierung geeigneter Backup- und Disaster-Recovery-Konzepte.

Corporate Manual Backup and Recovery Security Regulation (M60.02.08)

Spezifizierungen zu den Maßnahmen:

<input checked="" type="checkbox"/>	Unterbrechungsfreie Stromversorgung (USV)
<input checked="" type="checkbox"/>	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
<input checked="" type="checkbox"/>	Brand- und Rauchmeldesysteme
<input type="checkbox"/>	Alarmer bei unbefugten Zutritten zu Serverräumen
<input checked="" type="checkbox"/>	Tests zur Wiederherstellbarkeit von Daten
<input checked="" type="checkbox"/>	Aufbewahrung von Datensicherungen an einem separaten und sicheren Ort
<input type="checkbox"/>	In Hochwassergebieten: Serverräume oberhalb des Hochwasserspiegels
<input checked="" type="checkbox"/>	Klimageräte in Serverräumen
<input type="checkbox"/>	Geschützte Steckdosenleisten in Serverräumen
<input checked="" type="checkbox"/>	Feuerlöscher in Serverräumen
<input checked="" type="checkbox"/>	Erstellen eines Backup- & Recovery-Konzepts
<input type="checkbox"/>	Erstellen eines Notfallplans
<input type="checkbox"/>	Sonstige:

7. TRENNUNGSKONTROLLE/TRENNBARKEIT

Sicherstellung, dass Daten, die für unterschiedliche Zwecke erhoben werden, getrennt verarbeitet werden können (z.B. durch logische Trennung von Kundendaten, spezielle Zugriffskontrollen (Berechtigungskonzept), Trennung von Test- und Produktionsdaten).

Continental Information Security Guideline (CISG) – 3.5.1.4 Separation of development, test and operational facilities

Spezifizierungen zu den Maßnahmen:

<input checked="" type="checkbox"/>	Physisch getrennte Speicherung auf separaten Systemen oder Datenträgern
<input type="checkbox"/>	Einfügen von Zweckattributen/Datenfeldern in Datensätze
<input checked="" type="checkbox"/>	Festlegen von Datenbankrechten
<input type="checkbox"/>	Logische Kundentrennung (softwarebasiert)
<input type="checkbox"/>	Bei pseudonymisierten Daten: Trennung der Mapping-Datei und Speicherung auf einem separaten, gesicherten IT-System
<input checked="" type="checkbox"/>	Trennung von Produktions- und Testsystemen
<input type="checkbox"/>	Sonstige:

VDO FLEET ONLINE

**- ANNEX C "AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV) FÜR VDO FLEET SERVICES" -
(CONTINENTAL AFTERMARKET & SERVICES GMBH, VERSION 1.6, 04.07.2024)**

ANHANG 3 - UNTERAUFTRAGSVERARBEITER / INTERNATIONALE ÜBERMITTLUNGEN

Sicherstellung eines angemessenen Niveaus an technischen und organisatorischen Sicherheitsmaßnahmen bei den von CONTINENTAL beauftragten unterstützenden Parteien, um die relevanten personenbezogenen Daten in einem angemessenen und sicheren Rahmen verarbeiten zu können (Eignung von CONTINENTAL).

Werden Unterauftragsverarbeiter (z.B. für Hosting, Bereitstellung von Rechenzentrumsfläche, Betriebssoftware zur Verarbeitung personenbezogener Daten etc.) mit der Verarbeitung personenbezogener Daten beauftragt, ist die Umsetzung von technischen und organisatorischen Maßnahmen durch den jeweiligen Unterauftragsverarbeiter durch entsprechende Auftragsverarbeitungsvereinbarungen zu regeln. Der Unterauftragsverarbeiter stellt – bei ausreichender Gewährleistung – mindestens die mit CONTINENTAL vereinbarten technischen und organisatorischen Maßnahmen sicher.

Zur Verhinderung bzw. Vermeidung von unbefugten Zugriffen bzw. unbefugten Zugriffsversuchen auf die IT-Systeme und Speichereinrichtungen von CONTINENTAL einschließlich der dort gespeicherten Daten - sei es von außen oder von innen oder durch Auftragsverarbeiter - hat CONTINENTAL permanente Kontroll- und Überwachungsmaßnahmen für seine IT-Systeme einschließlich Zugangskontrolle/Zugangsüberwachung (24/7, 365 Tage) durch den Einsatz modernster Systeme/Firewalls/Zugangskontrolle etc. implementiert. Wird ein unbefugter Zugriff oder ein unbefugter Zugriffsversuch festgestellt, wird dieser automatisch und unverzüglich beendet. Das Service Team der Continental Automotive Technologies GmbH in Europa hat die ausschließliche Kontrolle über diese Sicherheitssysteme; ein Zugriff auf diese Systeme durch Verarbeiter oder andere ist ausgeschlossen.

Die folgenden Unterauftragsverarbeiter sind für die Bereitstellung von VDO FLEET Services durch CONTINENTAL eingebunden:

	<p>GILT NUR FÜR DEN FALL, DASS DIE CONTINENTAL AUTOMOTIVE TECHNOLOGIES GMBH NICHT DIREKTER VERTRAGSPARTNER DES KUNDEN IST UND ALS UNTERAUFTRAGSVERARBEITER VON <RSOS/NATIONALE HÄNDLER/PARTNER> AGIERT. (GILT FÜR ALLE LÄNDER/KUNDEN):</p>
<input checked="" type="checkbox"/>	<p>Continental Automotive Technologies GmbH, Vahrenwalder Straße 9, 30165 Hannover, Germany (Development and Support)</p>
	<p>UNTERAUFTRAGSVERARBEITER DER CONTINENTAL AUTOMOTIVE TECHNOLOGIES GMBH (GILT FÜR ALLE LÄNDER / KUNDEN):</p>
<input checked="" type="checkbox"/>	<p>Com-a-tec GmbH, Am Krebsgraben 15, 78048 Villingen-Schwenningen, Germany (Support Level 2)</p>
<input checked="" type="checkbox"/>	<p>Continental AG, Hauptverwaltung, Vahrenwalder Straße 9, D-30165 Hannover</p> <p>Die Continental AG ist Vertragsinhaberin über die Erbringung von Dienstleistungen durch den Unterauftragsverarbeiter der Continental AG gegenüber der Continental Automotive Technologies GmbH wie nachfolgend separat aufgeführt.</p>
<input checked="" type="checkbox"/>	<p>Continental Automotive Components (India) Private Limited Technical Center India, South Gate Tech Park, Plot No. 1, Veerasandra Industrial Area, Hosur Main Road, Bangalore - 560 100, India. Continental Automotive Components India ist ein Unternehmen der Continental-Gruppe, das Entwicklung, Überwachung und Unterstützung bei Dienstleistungen anbietet.</p> <p>Bitte beachten Sie: Jeder Zugriff von Continental Automotive Components India auf (personenbezogene) Daten von VDO Fleet-Kunden innerhalb des EWR unterliegt den Binding Corporate Rules der Continental-Gruppe, die ein angemessenes Datenschutzniveau im Sinne der Art. 45 ff. GDPR darstellen.</p>
<input checked="" type="checkbox"/>	<p>Continental Digital Services France SAS, 1 avenue Paul Ourliac B.P.13704 31037 Toulouse, France</p> <p>Continental Digital Services France ist ein Unternehmen der Continental-Gruppe, dass Entwicklung, Überwachung und Unterstützung für die Dienste anbietet.</p>
<input checked="" type="checkbox"/>	<p>Eviden Germany GmbH , Otto-Hahn Ring 6, 81739 München (Support und Wartung)</p>
<input checked="" type="checkbox"/>	<p>Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland (Anbieter von Cloud-Diensten, z. B. Google Cloud Platform)</p> <p>Bitte beachten Sie: Google wird als "Unterauftragsverarbeiter" für die Bereitstellung von Cloud-Diensten eingesetzt. In diesem Zusammenhang hat CONTINENTAL sichergestellt, dass die aus dem Europäischen Wirtschaftsraum (EWR) stammenden Daten nur innerhalb des EWR verarbeitet werden, es sei denn, es wurde etwas anderes mit dem KUNDEN vereinbart. Zusätzlich und hilfsweise gelten die Standardvertragsklauseln der EU-Kommission (wie im Durchführungsbeschluss (EU) 2021/914 der Kommission vom 04.06.2021 vorgesehen) sowie der neue Angemessenheitsbeschluss der EU-Kommission für die Datenverarbeitung in den USA vom 10.07.2023 für Google LLC. Darüber hinaus hat Continental, wie oben beschrieben, spezifische technische Sicherheitsmaßnahmen implementiert, um einen unbefugten Zugriff auf Daten, insbesondere von außerhalb des EWR, zu verhindern.</p>
<input checked="" type="checkbox"/>	<p>Kernel concepts GmbH, Hauptstraße 16, 57074 Siegen (Anbieter von Kernel-Diensten, Verbesserungen, Wartungen etc., Daten werden nur innerhalb des EWR verarbeitet)</p>
<input checked="" type="checkbox"/>	<p>Zonar Systems Inc., 18200 Cascade Ave S, Seattle, WA 98188, USA, eine hundertprozentige Tochtergesellschaft des Continental-Konzerns. Zonar Systems bietet Support-, Wartungs- und Entwicklungsdienstleistungen für die VDO Fleet-Services von Continental an.</p>

VDO FLEET ONLINE

**- ANNEX C "AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV) FÜR VDO FLEET SERVICES" -
(CONTINENTAL AFTERMARKET & SERVICES GMBH, VERSION 1.6, 04.07.2024)**

	<p>Bitte beachten Sie: Jeder Zugriff von Zonar Systems auf (personenbezogene) Daten des VDO Fleet-Kunden innerhalb des EWR unterliegt den Binding Corporate Rules des Continental-Konzerns, die ein angemessenes Datenschutzniveau im Sinne der Art 45 ff. DSGVO gewährleisten. Darüber hinaus wird der Zugang nur von Fall zu Fall gewährt, ist zeitlich begrenzt und wird kontinuierlich von der Sekretariatsabteilung der Continental Automotive Technologies GmbH in Europa kontrolliert/überwacht.</p> <p>Soweit Zonar Systems weitere Unterauftragsverarbeiter für die Erbringung seiner Dienstleistungen einsetzt, sind diese im Folgenden aufgeführt.</p>
--	--

	<p>UNTERAUFTRAGSVERARBEITER VON CONTINENTAL AUTOMOTIVE TRADING FRANCE SAS (GILT NUR FÜR FRANKREICH / FRANZÖSISCHE KUNDEN):</p>
<input checked="" type="checkbox"/>	<p>IMA TECHNOLOGIES, 31 Route de Gachet 44300 Nantes, France (Support Hotline)</p>

	<p>UNTERAUFTRAGSVERARBEITER DER CONTINENTAL AG (GILT FÜR ALLE LÄNDER / KUNDEN):</p>
<input checked="" type="checkbox"/>	<p>SYZYGY Deutschland GmbH, Im Atzelnest 3, 61352 Bad Homburg, Germany (Hosting-Dienstleistungen)</p>
<input checked="" type="checkbox"/>	<p>MongoDB Limited, Ireland, 3 Shelbourne Buildings, Ballsbridge, Dublin 4, Ireland (Anbieter von Cloud-Diensten; die Cloud-Dienste sind auf den EWR beschränkt)</p>

	<p>UNTERAUFTRAGSVERARBEITER VON ZONAR SYSTEMS, INC. (GILT FÜR ALLE LÄNDER / KUNDEN):</p>
<input checked="" type="checkbox"/>	<p>Clearblade Inc., 1701 Directors BLVD STE 250, Austin, TX 78744, USA (Lösung für die Verwaltung von Telematikverbindungen, Support / Wartung)</p> <p>Bitte beachten Sie: Continental hat sichergestellt, dass die Dienste und Daten, die aus dem EWR stammen, nur auf Servern im EWR verarbeitet werden. Darüber hinaus und als Ausweichmöglichkeit wurden die Standardvertragsklauseln der EU-Kommission (siehe Durchführungsbeschluss (EU) 2021/914 der Kommission vom 04.06.2021) mit Clearblade vereinbart. Darüber hinaus hat Continental, wie oben beschrieben, spezifische technische Sicherheitsmaßnahmen implementiert, um einen unbefugten Zugriff auf Daten, insbesondere von außerhalb des EWR, zu verhindern.</p>
<input checked="" type="checkbox"/>	<p>DataDog Inc., New York Times Bldg, 620 8th Ave 45th Floor, New York, MA, USA (Support & Verfügbarkeit)</p> <p>Bitte beachten Sie: Data Dog verarbeitet nur pseudonymisierte, aggregierte Daten; darüber hinaus und als Ersatz gelten die Standardvertragsklauseln der EU-Kommission (wie im Durchführungsbeschluss (EU) 2021/914 der Kommission vom 04.06.2021 vorgesehen). Darüber hinaus hat Continental, wie oben beschrieben, spezifische technische Sicherheitsmaßnahmen implementiert, um einen unbefugten Zugriff auf Daten, insbesondere von außerhalb des EWR, zu verhindern.</p>
<input checked="" type="checkbox"/>	<p>OKTA Inc., 100 First Street, 6th Floor, San Francisco, CA 94105, USA (Dienstleister Kundenidentitäts- und Zugangsmanagement (CIAM))</p> <p>Bitte beachten Sie: Continental hat sichergestellt, dass die Dienste und Daten, die aus dem EWR stammen, nur auf Servern innerhalb des EWR verarbeitet werden. Darüber hinaus und als Ausweichmöglichkeit wurden die Standardvertragsklauseln der EU-Kommission (siehe Durchführungsbeschluss (EU) 2021/914 der Kommission vom 04.06.2021) mit OKTA vereinbart, ebenso wie der neue Angemessenheitsbeschluss der EU-Kommission für die Datenverarbeitung in den USA vom 10.07.2023 gilt. Darüber hinaus hat Continental, wie oben beschrieben, spezifische technische Sicherheitsmaßnahmen implementiert, um einen unbefugten Zugriff auf Daten, insbesondere von außerhalb des EWR, zu verhindern.</p>
<input checked="" type="checkbox"/>	<p>MongoDB Limited, Ireland, 3 Shelbourne Buildings, Ballsbridge, Dublin 4, Ireland (Anbieter von Cloud-Diensten; die Cloud-Dienste sind auf den EWR beschränkt)</p>
<input checked="" type="checkbox"/>	<p>pendo.io Inc., 150 Fayetteville St., Raleigh, NC 27601, USA; European Representative (Art. 27 GDPR): DP-Dock GmbH, Ballindamm 39, 20095 Hamburg (Support & Entwicklung)</p> <p>Bitte beachten Sie: pendo.io verarbeitet nur pseudonymisierte, zusammengefasste. Die Daten werden nur innerhalb des EWR verarbeitet und gespeichert. Zusätzlich und als Fallback gelten die Standard-Vertragsklauseln der EU-Kommission (wie im Durchführungsbeschluss (EU) 2021/914 der Kommission vom 04.06.2021 vorgesehen). Darüber hinaus hat Continental, wie oben beschrieben, spezifische technische Sicherheitsmaßnahmen implementiert, um einen unbefugten Zugriff auf Daten, insbesondere von außerhalb des EWR, zu verhindern.</p>

<p>Allgemeine Informationen: Ihre Rechte im Rahmen der Europäischen Datenschutz-Grundverordnung bleiben unverändert. CONTINENTAL bestätigt ferner, dass Ihre Daten in Rechenzentren in der Europäischen Union gespeichert werden. CONTINENTAL verwendet höchste Sicherheitsstandards (z.B. ISO / DIN / HTTPS / Verschlüsselung) und schützt personenbezogene Daten bei der Übertragung und Speicherung.</p>
--