DATA PROCESSING AGREEMENT (DPA) FOR VDO FLEET-SERVICES (ANNEX D)

This DPA stipulates the legal obligations of the PARTIES regarding data protection resulting from the processing of personal data related to the respective contract about VDO FLEET SERVICES with the Customer. The following DPA is based on the official standard contractual terms established by the EU-Commission within the Commission's Implementing Decision (EU) 2021/915.

The Customer as "Controller" and CONTINENTAL AUTOMOTIVE TECHNOLOGIES GMBH as "Processor" agree as follows:

CLAUSE 1 Purpose and scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

b) The Controller(s) and Processor(s) as mentioned above have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

c) These Clauses apply to the processing of personal data as specified in Annex I.

d) Annexes I to III are an integral part of the Clauses.

e) These Clauses are without prejudice to obligations to which the Controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

CLAUSE 2 Invariability of the Clauses

GEGEVENSVERWERKERSOVEREENKOMST (DPA) VOOR VDO FLEET DIENSTEN (BIJLAGE D)

Deze DPA bepaalt de wettelijke verplichtingen van de PARTIJEN met betrekking tot gegevensbescherming als gevolg van de verwerking van persoonsgegevens met betrekking tot het respectieve contract over VDO FLEET SERVICES met de Klant. De volgende DPA is gebaseerd op de officiële standaard contractvoorwaarden die door de EU-Commissie zijn vastgesteld in Uitvoeringsbesluit (EU) 2021/915 van de Commissie.

De Klant als "Verwerkingsverantwoordelijke" en CONTINENTAL AUTOMOTIVE TECHNOLOGIES GMBH als "Verwerker" komen het volgende overeen:

ARTIKEL 1 Doel en scope

a) Het doel van deze standaard contractbepalingen (de clausules) is ervoor te zorgen dat wordt voldaan aan artikel 28, leden 3 en 4, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming).

b) De verwerkingsverantwoordelijke(n) en verwerker(s) zoals hierboven vermeld hebben ingestemd met deze clausules om naleving van artikel 28, leden 3 en 4, van Verordening (EU) 2016/679 en/of artikel 29 (3) en (4) Verordening (EU) 2018/1725.

c) Deze Clausules zijn van toepassing op de verwerking van persoonsgegevens zoals gespecificeerd in Bijlage I.

d) Bijlagen I tot III maken integraal deel uit van de clausules.

e) Deze clausules doen geen afbreuk aan de verplichtingen waaraan de Verantwoordelijke is onderworpen op grond van Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725.

f) Deze clausules garanderen op zichzelf niet de naleving van verplichtingen met betrekking tot internationale doorgiften in overeenstemming met hoofdstuk V van Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725.

ARTIKEL 2 Onveranderlijkheid van de clausules

a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

a) De partijen verbinden zich ertoe de clausules niet te wijzigen, behalve voor het toevoegen van informatie aan de bijlagen of het bijwerken van informatie daarin.

b) Dit belet de Partijen niet om de in deze clausules vastgelegde modelcontractbepalingen in een ruimer contract op te nemen, of andere clausules of aanvullende waarborgen toe te voegen, op voorwaarde dat deze niet direct of indirect in strijd zijn met de clausules of afbreuk doen aan de fundamentele rechten of vrijheden van betrokkenen.

CLAUSE 3 Interpretation

a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

ARTIKEL 3 Interpretatie

a) Wanneer in deze Clausules de termen worden gebruikt die zijn gedefinieerd in respectievelijk Verordening (EU) 2016/679 of Verordening (EU) 2018/1725, hebben die termen dezelfde betekenis als in die Verordening.

a) Deze clausules moeten worden gelezen en geïnterpreteerd in het licht van respectievelijk de bepalingen van Verordening (EU) 2016/679 of Verordening (EU) 2018/1725.

c) Deze clausules mogen niet worden geïnterpreteerd op een manier die in strijd is met de rechten en plichten voorzien in Verordening (EU) 2016/679 / Verordening (EU) 2018/1725 of op een manier die afbreuk doet aan de fundamentele rechten of vrijheden van de betrokkenen.

CLAUSE 4 Hierarchy / Order of Precedence

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

ARTIKEL 4 Hiërarchie/volgorde

In geval van tegenstrijdigheid tussen deze clausules en de bepalingen van daarmee verband houdende overeenkomsten tussen partijen die bestaan op het moment dat deze clausules worden overeengekomen of daarna worden aangegaan, gelden deze clausules.

CLAUSE 5 Docking clause

a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a Controller or a Processor by completing the Annexes and co-signing to this DPA.

b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a Controller or a Processor, in accordance with its co-signing.

c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

ARTIKEL 5 - Docking clausule

a) Elke entiteit die geen Partij binnen deze clausules kan, met instemming van alle partijen, te allen tijde als verwerkingsverantwoordelijke of verwerker toetreden tot deze clausules door de bijlagen in te vullen en mede te ondertekenen bij deze DPA.

b) Zodra de bijlagen in (a) zijn ingevuld en ondertekend, wordt de toetredende entiteit, als mede ondertekenaar, behandeld als een Partij bij deze clausules en heeft zij de rechten en verplichtingen van een verwerkingsverantwoordelijke of een verwerker.

c) De toetredende entiteit heeft geen rechten of verplichtingen die voortvloeien uit deze clausules uit de periode voorafgaand aan de toetreding van Partij.

SECTION II
OBLIGATIONS OF THE PARTIES

Sectie II
VERPLICHTINGEN VAN DE PARTIJEN

CLAUSE 6 Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Controller, are specified in Annex I.

ARTIKEL 6 Beschrijving van de verwerking(en)

De details van de verwerkingen, met name de categorieën persoonsgegevens en de doeleinden van de verwerking waarvoor de persoonsgegevens namens de Verantwoordelijke worden verwerkt, zijn gespecificeerd in bijlage I.

CLAUSE 7 Obligations of the Parties

7.1. Instructions

a) The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe Regulation (EU) 2016/679 / Regulation (EU)

ARTIKEL 7 Verplichtingen van de partijen

7.1. instructies:

a) De Verwerker zal persoonsgegevens alleen verwerken op gedocumenteerde instructies van de Verwerkingsverantwoordelijke, tenzij dit wordt vereist door de Unie- of Lidstatenwetgeving waaraan de Verwerker is onderworpen. In dat geval zal Verwerker Verwerkingsverantwoordelijke voorafgaand aan de verwerking op de hoogte stellen van die wettelijke verplichting, tenzij de wet dit verbiedt op zwaarwegende gronden van algemeen belang. Verdere instructies kunnen ook door de Verantwoordelijke worden gegeven gedurende de duur van de verwerking van persoonsgegevens. Deze instructies moeten altijd worden gedocumenteerd.

7.2. doel beperking

Verwerker zal de persoonsgegevens alleen verwerken voor de specifieke doeleinden van de

2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The Processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex I, unless it receives further instructions from the Controller.

7.3. Duration of the processing of personal data

Processing by the Processor shall only take place for the duration specified in Annex I.

7.4. Security of processing

a) The Processor shall at least implement the technical and organizational measures specified in Annex II to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

b) The Processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The Processor shall ensure that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the Processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The Processor shall deal promptly and adequately with inquiries from the Controller about the

verwerking, zoals uiteengezet in Bijlage I, tenzij hij nadere instructies ontvangt van Verantwoordelijke.

7.3. Duur van de verwerking van persoonsgegevens

Verwerking door Verwerker vindt alleen plaats voor de in Bijlage I genoemde duur.

7.4. Beveiliging van verwerking

a) Verwerker zal in ieder geval de in Bijlage II genoemde technische en organisatorische maatregelen treffen om de beveiliging van de persoonsgegevens te waarborgen. Dit omvat het beschermen van de gegevens tegen inbreuken op de beveiliging die leiden tot onopzettelijke of onwettige vernietiging, verlies, wijziging, ongeoorloofde openbaarmaking of toegang tot de gegevens (inbreuk in verband met persoonsgegevens). Partijen houden bij de beoordeling van het passende beveiligingsniveau rekening met de stand van de techniek, de uitvoeringskosten, de aard, omvang, context en doeleinden van de verwerking en de risico's voor de betrokkenen.

b) De verwerker zal zijn personeel alleen toegang verlenen tot de persoonsgegevens die worden verwerkt voor zover dit strikt noodzakelijk is voor de uitvoering, het beheer en de controle van het contract. Verwerker draagt er zorg voor dat personen die bevoegd zijn om de ontvangen persoonsgegevens te verwerken zich tot geheimhouding hebben verplicht of data verwerken volgens een wettelijke procedure tot verplichting tot geheimhouding.

7.5. Gevoelige data

Als de verwerking betrekking heeft op persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of lidmaatschap van een vakbond blijken, genetische gegevens of biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, gegevens over de gezondheid of iemands seksleven of seksuele oriëntatie, of gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten ("gevoelige gegevens"), zal de Verwerker specifieke beperkingen en/of aanvullende veiligheden toepassen.

7.6 Documentatie en naleving

a) Partijen kunnen aantonen dat ze aan deze clausules voldoen.

b) Verwerker zal vragen van Verantwoordelijke over de verwerking van gegevens in overeenstemming met deze Clausules prompt en adequaat behandelen.

processing of data in accordance with these Clauses.

c) The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the Controller's request, the Processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Controller may take into account relevant certifications held by the Processor.

d) The Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Processor and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of Sub-Processors

a) The Processor has the Controller's general authorization for the engagement of sub-Processors from an agreed list. The Processor shall specifically inform in writing the Controller of any intended changes of that list through the addition or replacement of sub-Processors at least 30 (thirty) days in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-Processor(s). The Processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object. If the Controller does not object within 30 days, his respective consent shall be deemed granted.

The Controller agrees herewith with the involvement of the Sub-Processors as listed in Annex III.

b) Where the Processor engages a sub-Processor for carrying out specific processing activities (on behalf of the Controller), it shall do so by way of a contract which imposes on the sub-Processor, in substance, the same data protection obligations as the ones imposed on the data Processor in accordance with these Clauses. The Processor

c) Verwerker stelt Verantwoordelijke alle informatie ter beschikking die nodig is om aan te tonen dat wordt voldaan aan de verplichtingen die in deze Clausules zijn uiteengezet en die rechtstreeks voortvloeien uit Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725. Op verzoek van Verantwoordelijke zal Verwerker ook met redelijke tussenpozen of bij aanwijzingen van niet-naleving audits van de onder deze Artikelen vallende verwerkingen toestaan en hieraan bijdragen. Bij het nemen van een beslissing over een review of een audit kan de Verantwoordelijke rekening houden met relevante certificeringen van de Verwerker.

d) De Verwerkingsverantwoordelijke kan ervoor kiezen de audit zelf uit te voeren of een onafhankelijke auditor te machtigen. Audits kunnen ook inspecties in de gebouwen of fysieke faciliteiten van de Verwerker omvatten en zullen, indien van toepassing, worden uitgevoerd met een voorafgaande aankondiging met een redelijke termijn.

d) Partijen stellen de in dit artikel bedoelde informatie, inclusief de resultaten van eventuele audits, op verzoek ter beschikking aan de bevoegde toezichthoudende autoriteit(en).

7.7 Gebruik van subprocessen

a) Verwerker heeft de algemene machtiging van Verantwoordelijke voor het inschakelen van subverwerkers uit een overeengekomen lijst. Verwerker zal Verantwoordelijke uitdrukkelijk schriftelijk informeren over eventuele voorgenomen wijzigingen van die lijst door toevoeging of vervanging van subverwerkers, ten minste 30 (dertig) dagen van tevoren, zodat Verantwoordelijke voldoende tijd heeft om bezwaar te kunnen maken tegen dergelijke wijzigingen voordat aan de inschakeling van de betrokken subverwerker(s). Verwerker zal Verantwoordelijke de informatie verstrekken die nodig is om Verantwoordelijke in staat te stellen het recht van bezwaar uit te oefenen.

shall ensure that the sub-Processor complies with the obligations to which the Processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) At the Controller's request, the Processor shall provide a copy of such a sub-Processor agreement and any subsequent amendments to the Controller. To the extent necessary to protect business secret or other confidential information, including personal data, the Processor may redact the text of the agreement prior to sharing the copy.

d) The Processor shall remain fully responsible to the Controller for the performance of the sub-Processor's obligations in accordance with its contract with the Processor. The Processor shall notify the Controller of any failure by the sub-Processor to fulfil its contractual obligations.

7.8. International data transfers / international data processing

a) Any transfer of data to a third country or an international organization by the Processor shall be done - notwithstanding the provision in lit b below – only,
   i. on the basis of documented instructions,
   ii. on the basis of a prior (general) consent by the Controller or
   iii. in order to fulfil a specific requirement under Union or Member State law to which the Processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) Where the Processor engages a sub-Processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the Controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the Controller agrees that such processing is allowed provided that

   i. the processing will be conducted in a country for which the EU-Commission has adopted a respective adequacy decision on the basis of Article 45 of Regulation (EU) 2016/679, or

   ii. the Processor and the Sub-Processor ensure compliance with Chapter V of Regulation

Als de verwerkingsverantwoordelijke niet binnen 30 dagen bezwaar maakt, wordt zijn respectieve toestemming geacht te zijn verleend.

Verwerkingsverantwoordelijke stemt hierbij in met de betrokkenheid van de Subverwerkers zoals vermeld in Bijlage III.

c) Wanneer de verwerker een subverwerker inschakelt voor het uitvoeren van specifieke verwerkingsactiviteiten (namens de controller), zal hij dit doen door middel van een contract dat de subverwerker in wezen dezelfde verplichtingen inzake gegevensbescherming oplegt als die welke in overeenstemming met deze clausules aan de gegevensverwerker zijn opgelegd. Verwerker zorgt ervoor dat de subverwerker voldoet aan de verplichtingen die op Verwerker rusten op grond van deze Artikelen en Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725.

c) Op verzoek van Verantwoordelijke verstrekt Verwerker een kopie van een dergelijke sub-verwerkersovereenkomst en eventuele latere wijzigingen aan Verantwoordelijke. Voor zover nodig ter bescherming van bedrijfsgeheimen of andere vertrouwelijke informatie, waaronder persoonsgegevens, kan Verwerker de tekst van de overeenkomst redigeren voordat de kopie wordt gedeeld.

d) De Verwerker blijft volledig verantwoordelijk jegens de Verantwoordelijke voor de uitvoering van de verplichtingen van de sub-verwerker in overeenstemming met zijn contract met de Verwerker. De Verwerker zal de Verwerkingsverantwoordelijke op de hoogte stellen van elk verzuim door de subverwerker om zijn contractuele verplichtingen na te komen.

7.8. Internationale gegevensoverdracht / internationale gegevensverwerking

a) Elke overdracht van gegevens aan een derde land of een internationale organisatie door de Verwerker zal - niettegenstaande het bepaalde in lid b) hieronder - alleen gebeuren:
   i. op basis van gedocumenteerde instructies,
   ii. op basis van een voorafgaande (algemene) toestemming van de Verantwoordelijke of
   iii. om te voldoen aan een specifieke vereiste op grond van het Unie- of lidstaatrecht waaraan de Verwerker is onderworpen en zal plaatsvinden in overeenstemming met Hoofdstuk V van Verordening (EU) 2016/679 of Verordening (EU) 2018/1725.

b) Indien de verwerker een subverwerker inschakelt in overeenstemming met artikel 7.7. voor het uitvoeren

(EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

c) The Controller agrees herewith with the transfer and processing of personal data within the meaning of Chapter V of Regulation (EU) 2016/679 by the Processor and/or Sub-Processors as listed in Annex III.

van specifieke verwerkingsactiviteiten (namens de Verantwoordelijke) en die verwerkingsactiviteiten een doorgifte van persoonsgegevens in de zin van hoofdstuk V van Verordening (EU) 2016/679 inhouden, stemt de Verantwoordelijke ermee in dat een dergelijke verwerking is toegestaan op voorwaarde dat

i. de verwerking zal plaatsvinden in een land waarvoor de EU-Commissie een respectief adequaatheidsbesluit heeft genomen op basis van artikel 45 van Verordening (EU) 2016/679, of

ii. de verwerker en de subverwerker zorgen voor naleving van hoofdstuk V van Verordening (EU) 2016/679 door gebruik te maken van modelcontractbepalingen die door de Commissie zijn aangenomen in overeenstemming met artikel 46, lid 2, van Verordening (EU) 2016/679, op voorwaarde dat de voorwaarden voor het gebruik van die modelcontractbepalingen is voldaan.

c) Verantwoordelijke stemt hiermee in met de doorgifte en verwerking van persoonsgegevens in de zin van Hoofdstuk V van Verordening (EU) 2016/679 door Verwerker en/of Subverwerkers zoals vermeld in Bijlage III.

CLAUSE 8 Assistance to the Controller

a) The Processor shall promptly notify the Controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorized to do so by the Controller.

b) The Processor shall assist the Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the Processor shall comply with the Controller's instructions

c) In addition to the Processor's obligation to assist the Controller pursuant to Clause 8(b), the Processor shall furthermore assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the Processor:

   i. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

   ii. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

   iii. the obligation to ensure that personal data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

   iv. the obligations in Article 32 Regulation (EU) 2016/679.

d) The Parties shall set out in Annex II the appropriate technical and organizational measures by which the Processor is required to assist the Controller in the application of this Clause as well as the scope and the extent of the assistance required.

ARTIKEL 8 Assistentie aan de Verwerkingsverantwoordelijke

a) De Verwerker stelt de Verantwoordelijke direct op de hoogte van elk verzoek dat hij van de betrokkene heeft ontvangen. Zij zal niet zelf op het verzoek reageren, tenzij hiervoor toestemming is verleend door de Verwerkingsverantwoordelijke.

b) De Verwerker helpt de Verantwoordelijke bij het nakomen van zijn verplichtingen om te reageren op verzoeken van betrokkenen om hun rechten uit te oefenen, rekening houdend met de aard van de verwerking. Bij het nakomen van zijn verplichtingen conform (a) en (b) zal Verwerker de instructies van Verantwoordelijke opvolgen

c) Naast de verplichting van de Verwerker om de Verantwoordelijke bij te staan op grond van artikel 8(b), zal de Verwerker de Verantwoordelijke verder assisteren bij het nakomen van de volgende verplichtingen, rekening houdend met de aard van de gegevensverwerking en de informatie waarover de verwerker:

   i. de verplichting om een beoordeling uit te voeren van de impact van de beoogde verwerkingen op de bescherming van persoonsgegevens (een 'gegevensbeschermingseffectbeoordeling') wanneer een type verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen;

   iii. de verplichting om voorafgaand aan de verwerking de bevoegde toezichthoudende autoriteit(en) te raadplegen wanneer uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico met zich meebrengt als de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken;

   iii. de verplichting om ervoor te zorgen dat persoonsgegevens juist en up-to-date zijn, door Verwerkingsverantwoordelijke onverwijld op de hoogte te stellen als Verwerker vaststelt dat de door hem verwerkte persoonsgegevens onjuist of verouderd zijn;

   iv. de verplichtingen in artikel 32 Verordening (EU) 2016/679.

d) Partijen stellen in Bijlage II de passende technische en organisatorische maatregelen vast waarmee Verwerker de Verwerkingsverantwoordelijke dient bij te staan bij de toepassing van dit artikel, alsmede de scope en omvang van de benodigde assistentie.

CLAUSE 9 Notification of personal data breach

In the event of a personal data breach, the Processor shall cooperate with and assist the Controller for the Controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the Processor.

9.1 Data breach concerning data processed by the Controller

In the event of a personal data breach concerning data processed by the Controller, the Processor shall assist the Controller:

a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the Controller has become aware of it, where relevant/ (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the Controller's notification, and must at least include:

i. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

ii. the likely consequences of the personal data breach;

iii. the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the

ARTIKEL 9 Melding van inbreuk van persoonsgegevens

In het geval van een inbreuk in verband met persoonsgegevens, zal de Verwerker samenwerken met en assisteren van de Verantwoordelijke voor de Verantwoordelijke om te voldoen aan zijn verplichtingen op grond van de artikelen 33 en 34 Verordening (EU) 2016/679 of op grond van de artikelen 34 en 35 Verordening (EU) 2018/ 1725, indien van toepassing, rekening houdend met de aard van de verwerking en de informatie waarover de Verwerker beschikt.

9.1 Datalek betreffende gegevens verwerkt door Verwerkingsverantwoordelijke

In het geval van een inbreuk van persoonsgegevens met betrekking tot door Verantwoordelijke verwerkte gegevens, staat Verwerker Verantwoordelijke bij:

a) bij het melden van de inbreuk van persoonsgegevens aan de bevoegde toezichthoudende autoriteit(en), zonder onnodige vertraging nadat de verwerkingsverantwoordelijke er kennis van heeft genomen, indien relevant/ (tenzij het onwaarschijnlijk is dat de inbreuk van persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen);

b) bij het verkrijgen van de volgende informatie die, op grond van artikel 33, lid 3, Verordening (EU) 2016/679, moet worden vermeld in de kennisgeving van de verwerkingsverantwoordelijke, en die ten minste moet bevatten:

i. de aard van de persoonsgegevens, inclusief waar mogelijk, de categorieën en het geschatte aantal betrokken betrokkenen en de categorieën en het geschatte aantal bestanden met persoonsgegevens;

ii. de waarschijnlijke gevolgen van de inbreuk van persoonsgegevens;

iii. de maatregelen die de Verwerkingsverantwoordelijke heeft genomen of voorgesteld te nemen om de inbreuk van persoonsgegevens aan te pakken, met inbegrip van, in voorkomend geval, maatregelen om de mogelijke nadelige gevolgen ervan te beperken.

Indien, en voor zover het niet mogelijk is, om al deze informatie tegelijkertijd te verstrekken, bevat de eerste kennisgeving de informatie die op dat moment beschikbaar is en wordt verdere informatie, zodra deze beschikbaar komt, direct verstrekt.

d) bij het voldoen, overeenkomstig artikel 34 van Verordening (EU) 2016/679, aan de verplichting om de

personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the Processor

In the event of a personal data breach concerning data processed by the Processor, the Processor shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex II all other elements to be provided by the Processor when assisting the Controller in the compliance with the Controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

inbreuk van persoonsgegevens direct mede te delen aan de betrokkene, wanneer de inbreuk van persoonsgegevens waarschijnlijk zal leiden tot een hoog risico voor de rechten en vrijheden van natuurlijke personen.

9.2 Datalek betreffende gegevens verwerkt door Verwerker

In geval van een inbreuk van persoonsgegevens met betrekking tot door Verwerker verwerkte gegevens, stelt Verwerker Verantwoordelijke direct op de hoogte nadat Verwerker kennis heeft gekregen van de inbreuk. Een dergelijke kennisgeving bevat ten minste:

a) een beschrijving van de aard van de inbreuk (inclusief, waar mogelijk, de categorieën en het geschatte aantal betrokken personen en gegevensbestanden);

b) de gegevens van een contactpunt waar meer informatie over de inbreuk in verband met persoonsgegevens kan worden verkregen;

c) de waarschijnlijke gevolgen en de maatregelen die zijn genomen of worden voorgesteld om de inbreuk aan te pakken, met inbegrip van de mogelijke nadelige gevolgen ervan.

Indien en voor zover het niet mogelijk is om al deze informatie tegelijkertijd te verstrekken, bevat de eerste kennisgeving de informatie die op dat moment beschikbaar is en wordt verdere informatie, zodra deze beschikbaar komt, direct verstrekt.

De Partijen zetten in Bijlage II alle andere elementen uiteen die door de Verwerker moeten worden verstrekt bij het assisteren van de Verwerkingsverantwoordelijke bij de naleving van de verplichtingen van de Verwerkingsverantwoordelijke op grond van de artikelen 33 en 34 van Verordening (EU) 2016/679.

SECTION III
FINAL PROVISIONS

CLAUSE 10 Non-compliance with the Clauses and termination

a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the Processor is in breach of its obligations under these Clauses, the Controller may instruct the Processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The Processor shall promptly inform

SECTIE III
SLOTBEPALINGEN

ARTIKEL 10 Niet-naleving van de clausules en beëindiging

a) Onverminderd het bepaalde in Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725, kan Verwerker in het geval Verwerker zijn verplichtingen op grond van deze Artikelen niet nakomt, Verwerkingsverantwoordelijke opdracht geven tot het opschorting van de verwerking van persoonsgegevens totdat deze aan deze clausules voldoet of het contract wordt beëindigd. Verwerker zal Verwerkingsverantwoordelijke direct informeren

the Controller in case it is unable to comply with these Clauses, for whatever reason.

b) The Controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

i. the processing of personal data by the Processor has been suspended by the Controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

ii. the Processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

iii. the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The Processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the Controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the Controller insists on compliance with the instructions.

d) Following termination of the contract, the Processor shall, at the choice of the Controller, delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so, or return all the personal data to the Controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the Processor shall continue to ensure compliance with these Clauses.

CLAUSE 11 LIST OF APPENDICES

APPENDIX 1: Details of Processing
APPENDIX 2: Technical and organizational measures for contract data processing implemented by CONTINENTAL.

indien hij om welke reden dan ook niet aan deze Artikelen kan voldoen.

b) De verwerkingsverantwoordelijke heeft het recht om het contract te beëindigen voor zover het de verwerking van persoonsgegevens in overeenstemming met deze clausules betreft, indien:

i. de verwerking van persoonsgegevens door de Verwerker door de Verantwoordelijke is opgeschort op grond van punt (a) en als de naleving van deze Clausules niet binnen een redelijke termijn en in ieder geval binnen een maand na de beëindiging wordt hersteld;

ii. de Verwerker schendt in substantiële wijze of bij voortdurende schending van deze Clausules en/of zijn verplichtingen onder Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725;

iii. de Verwerker voldoet niet aan een bindende uitspraak van een bevoegde rechter of de bevoegde toezichthoudende autoriteit(en) met betrekking tot zijn verplichtingen op grond van deze Clausules of Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725.

c) De Verwerker heeft het recht om het contract te beëindigen voor zover het de verwerking van persoonsgegevens onder deze Clausules betreft, indien de Controller, na de Verwerkingsverantwoordelijke te hebben geïnformeerd dat zijn instructies in strijd zijn met de toepasselijke wettelijke vereisten in overeenstemming met Clausule 7.1 (b), aandringt op naleving van de instructies.

d) Na beëindiging van de overeenkomst zal Verwerker, naar keuze van Verwerkingsverantwoordelijke, alle in opdracht van Verwerkingsverantwoordelijke verwerkte persoonsgegevens verwijderen en aan Verwerkingsverantwoordelijke verklaren dat hij dit heeft gedaan, dan wel alle persoonsgegevens aan Verwerkingsverantwoordelijke teruggeven en bestaande kopieën verwijderen, tenzij het recht van de Unie of de lidstaten de opslag van de persoonsgegevens vereist. Totdat de gegevens worden verwijderd of geretourneerd, blijft Verwerker toezien op de naleving van deze Clausules.

ARTIKEL 11 Lijst van bijlagen

APPENDIX 1: Details van de verwerking
APPENDIX 2: Technische en organisatorische maatregelen ter bescherming van persoonsgegevens onder de werking van de DPA, geïmplementeerd door CONTINENTAL.

APPENDIX 3:	Subcontractor	APPENDIX 3:	Sub-verwerkers

APPENDIX I - DESCRIPTION OF PROCESSING

1. PURPOSE(S) FOR WHICH THE PERSONAL DATA IS PROCESSED ON BEHALF OF THE CONTROLLER

CONTINENTAL instructed to act as a data processor, in order to process on behalf of CUSTOMER (the Controller) the personal data which are necessary to render the services of the VDO FLEET SERVICES.

2. MANNER AND PURPOSE OF THE DATA PROCESSING IS:

2.1 CONTINENTAL is entitled to collect, process and use personal data only in accordance with the TIS WEB Services CONTRACT and the instructions of the CUSTOMER (see Clause 7.1).

2.2 Details on the scope, nature and purpose of the collection, processing and / or use of personal data is subject of the General Terms and Conditions of the Main Contract, its Service Description as well as the products' functional overviews.

3. CATEGORIES OF DATA SUBJECTS:

- ☒ CUSTOMERs
- ☐ Visitors
- ☐ Event participants
- ☒ Service users
- ☒ Communication participants
- ☒ Subscribers
- ☐ Interested parties
- ☐ Supplier and/ or Service Provider (individual contacts at these vendors)
- ☒ Employees
- ☐ Applicants
- ☐ Former employees
- ☐ Apprentices/ interns
- ☐ Employees relatives
- ☐ Consultants
- ☒ Sales representatives
- ☐ Shareholders / bodies
- ☒ Contact persons for business
- ☐ Suppliers and service providers
- ☒ Business partners
- ☒ Other please specify: those employed by customers; i. e. drivers and users of VDO FLEET-SERVICES

BIJLAGE I - BESCHRIJVING VAN VERWERKING

1. DOEL(EN) WAARVOOR DE PERSOONSGEGEVENS NAMENS DE VERANTWOORDELIJKE WORDEN VERWERKT

CONTINENTAL heeft opdracht gekregen om als gegevensverwerker op te treden om namens KLANT (de Verantwoordelijke) de persoonsgegevens te verwerken die nodig zijn om de diensten van de VDO FLEET DIENSTEN te verlenen.

2. WIJZE EN DOEL VAN DE GEGEVENSVERWERKING IS:

2.1 CONTINENTAL heeft het recht om persoonsgegevens alleen te verzamelen, verwerken en gebruiken in overeenstemming met het TIS WEB Services-CONTRACT en de instructies van de KLANT (zie Artikel 7.1).

2.2 Details over de omvang, aard en het doel van het verzamelen, verwerken en/of gebruiken van persoonsgegevens zijn onderworpen aan de Algemene Voorwaarden van het Hoofdcontract, de Servicebeschrijving en de functionele overzichten van de producten.

3. CATEGORIES OF DATA SUBJECTS:

- ☒ CUSTOMERs
- ☐ Visitors
- ☐ Event participants
- ☒ Service users
- ☒ Communication participants
- ☒ Subscribers
- ☐ Interested parties
- ☐ Supplier and/ or Service Provider (individual contacts at these vendors)
- ☒ Employees
- ☐ Applicants
- ☐ Former employees
- ☐ Apprentices/ interns
- ☐ Employees relatives
- ☐ Consultants
- ☒ Sales representatives
- ☐ Shareholders / bodies
- ☒ Contact persons for business
- ☐ Suppliers and service providers
- ☒ Business partners
- ☒ Other please specify: those employed by customers; i. e. drivers and users of VDO FLEET DIENSTEN

4. TYPE OF PERSONAL DATA

General data/ private contact details

☒ Names Personal profiles
☐ Image
☒ Private address data
☒ Date of birth
☒ ID card data (e.g. Passport, Social Security, Driving License)
☐ Other please specify:

_____

Contract data

☒ Settlement and payment data
☒ Bank details/ credit card data
☒ Financial Standing/ Creditworthiness
☒ Contract histories
☐ Other please specify:

_____

Professional data

☒ Personal Details
☐ Position and Employment Details
☒ Performance Management
☐ Qualification and Education Details
☒ Social Security Data
☒ Absence from Work
☒ Other please specify:

- admission data of the customer and its operators / users
- driver data (e. g. name, address (company or private address as applicable), gender, birthday, licence number, card number etc.)
- vehicle data and vehicle profiles
- communications data (e. g. telephone, email)
- movement data, GPS data
- activities of drivers and deployment profile, including driving times and rest times in accordance with Attachment 1B of the Regulation (EU) No. 561/2006, Regulation (EU) No. 2020/1054, Regulation (EC) No. 1360/2002, Regulation No. 165/2014 and Implementing Regulation (EU) No. 2016/799.

4. TYPE OF PERSONAL DATA

General data/ private contact details

☒ Names Personal profiles
☐ Image
☒ Private address data
☒ Date of birth
☒ ID card data (e.g. Passport, Social Security, Driving License)
☐ Other please specify:

_____

Contract data

☒ Settlement and payment data
☒ Bank details/ credit card data
☒ Financial Standing/ Creditworthiness
☒ Contract histories
☐ Other please specify:

_____

Professional data

☒ Personal Details
☐ Position and Employment Details
☒ Performance Management
☐ Qualification and Education Details
☒ Social Security Data
☒ Absence from Work
☒ Other please specify:

- admission data of the customer and its operators / users
- driver data (e. g. name, address (company or private address as applicable), gender, birthday, licence number, card number etc.)
- vehicle data and vehicle profiles
- communications data (e. g. telephone, email)
- movement data, GPS data
- activities of drivers and deployment profile, including driving times and rest times in accordance with Attachment 1B of the Regulation (EU) No. 561/2006, Regulation (EU) No. 2020/1054, Regulation (EC) No. 1360/2002, Regulation No. 165/2014 and Implementing Regulation (EU) No. 2016/799.

- data for use of the service by users download data for the driver card and tachograph

Service and IT usage data

- ☐ Device identifiers
- ☒ Usage and connection data
- ☐ Image / video data
- ☒ Telecommunication data/ message content
- ☐ Audio / voice data
- ☐ Identification data
- ☒ Access data
- ☐ Authorization
- ☐ Meta data
- ☐ Other please specify:

_____

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Special categories of personal data

- ☐ Race or Ethnic Origin
- ☐ Religious or Philosophical Beliefs
- ☐ Physical or Mental Health
- ☐ Political Opinions
- ☐ Biometric Data
- ☐ Genetic Data
- ☐ Trade Union Membership
- ☐ Sexual Life
- ☐ Criminal Offences, Convictions or Judgments
- ☐ Other please specify:

_____

- data for use of the service by users download data for the driver card and tachograph

Service and IT usage data

- ☐ Device identifiers
- ☒ Usage and connection data
- ☐ Image / video data
- ☒ Telecommunication data/ message content
- ☐ Audio / voice data
- ☐ Identification data
- ☒ Access data
- ☐ Authorization
- ☐ Meta data
- ☐ Other please specify:

_____

Gevoelige gegevens die worden verwerkt (indien van toepassing) en toegepaste beperkingen of beveiligingen die volledig rekening houden met de aard van de gegevens en de bijbehorende risico's, zoals bijvoorbeeld strikte doelbinding, toegangsbeperkingen (inclusief toegang alleen voor personeel dat een gespecialiseerde opleiding heeft gevolgd), bewaren een registratie van toegang tot de gegevens, beperkingen voor verdere doorgifte of aanvullende veiligheidsmaatregelen.

Special categories of personal data

- ☐ Race or Ethnic Origin
- ☐ Religious or Philosophical Beliefs
- ☐ Physical or Mental Health
- ☐ Political Opinions
- ☐ Biometric Data
- ☐ Genetic Data
- ☐ Trade Union Membership
- ☐ Sexual Life
- ☐ Criminal Offences, Convictions or Judgments
- ☐ Other please specify:

_____

5. DURATION OF THE PROCESSING

5.1 The duration of the data processing depends on the term of the Contract and/or any individual contracts or orders based on a framework agreement.

5.2 Until completion of the processing and subject to any other documented instructions of the Controller, the Processor shall return to the Controller or to a third party designated by the Controller, all documents, data carriers, processing results and data which have come into its possession, and which are connected with the contractual relationship or have been generated in the course of the execution of the Contract and/or this DPA.
This obligation extends to copies and/or reproductions of data carriers and/or data stocks. There is no right of retention with regard to the aforementioned data and data carriers. Unless otherwise provided for in the Contract, the Processor shall return all data and data carriers to the Controller free of charge. The Processor shall bear any costs and other expenses in connection with the return of data.

5.3 The Controller cannot demand the deletion of the data stored by the Processor, if and to the extent the Processor is subject to statutory retention obligations. Instead of deletion, the processing of the data can be restricted, as far as this is permissible due to local / country-specific implementation laws on data protection. This applies in particular if, due to the specific storage method, the deletion is not possible or only possible with disproportionately high expenditure.

5. DUUR VAN DE VERWERKING

5.1 De duur van de gegevensverwerking is afhankelijk van de looptijd van het Contract en/of eventuele individuele contracten of opdrachten op basis van een raamovereenkomst.

5.2 Totdat de verwerking is voltooid en behoudens eventuele andere gedocumenteerde instructies van Verantwoordelijke, zal Verwerker alle in haar bezit gekomen documenten, gegevensdragers, verwerkingsresultaten en gegevens aan Verantwoordelijke of aan een door Verantwoordelijke aangewezen derde retourneren , en die verband houden met de contractuele relatie of zijn gegenereerd in de loop van de uitvoering van het Contract en/of deze DPA.
Deze verplichting strekt zich uit tot kopieën en/of reproducties van gegevensdragers en/of gegevensbestanden. Ten aanzien van voornoemde gegevens en gegevensdragers bestaat geen retentierecht. Tenzij in de Overeenkomst anders is bepaald, zal Verwerker alle gegevens en gegevensdragers kosteloos aan Verwerkingsverantwoordelijke retourneren. Verwerker draagt alle kosten en andere uitgaven in verband met het retourneren van gegevens.

5.3 Verwerkingsverantwoordelijke kan de verwijdering van de door Verwerker opgeslagen gegevens niet verlangen, indien en voor zover op Verwerker wettelijke bewaarplichten rusten. In plaats van verwijdering kan de verwerking van de gegevens worden beperkt, voor zover dit op grond van lokale/landspecifieke uitvoeringswetten inzake gegevensbescherming is toegestaan. Dit geldt in het bijzonder als de verwijdering door de specifieke opslagmethode niet of met onevenredig hoge kosten mogelijk is.

APPENDIX II - TECHNICAL AND ORGANIZATIONAL MEASURES

1. PHYSICAL ACCESS CONTROL

The Corporate Policy Continental Information Security Guideline (CISG) defines the **minimum requirements** for technical and organizational measures at CONTINENTAL in dealing with information. Depending on the classification of the information, measures are implemented that go beyond the minimum requirements.

The requirements of the CISG are implemented in the company on the basis of the Corporate Standard Information Security Framework and the corresponding Information Security Management System (ISMS).

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

Specifications for the measures:

☒	Alarm system
☒	Automatic access control system
☐	Locking system with code lock
☐	Biometric access barriers
☐	Light barriers/motion sensors
☒	Manual locking system including key regulation (key book, key issue)
☒	Visitor logging
☒	Careful selection of security staff
☒	Chip cards/transponder locking systems
☒	Video monitoring of access doors
☒	Safety locks
☒	Personnel screening by gatekeeper/reception
☒	Careful selection of cleaning staff
☒	Obligation to wear employee/guest ID cards
☐	Other:

BIJLAGE II – TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

1. FYSIEKE TOEGANGSCONTROLE

De Corporate Policy Continental Information Security Guideline (CISG) definieert de minimumvereisten voor technische en organisatorische maatregelen bij CONTINENTAL in de omgang met informatie. Afhankelijk van de classificatie van de informatie worden maatregelen genomen die verder gaan dan de minimumeisen. De eisen van het CISG worden in het bedrijf geïmplementeerd op basis van het Corporate Standard Information Security Framework en het bijbehorende Information Security Management System (ISMS).

Bedrijfsbeleid Continentale informatiebeveiligingsrichtlijn (CISG)
Corporate Standard Information Security Framework
Bijlage 1 - Managementsysteem voor informatiebeveiliging (ISMS)
Bijlage 2 - Rollen en verantwoordelijkheden in informatiebeveiliging - RACI Chart

Specifications for the measures:

☒	Alarm system
☒	Automatic access control system
☐	Locking system with code lock
☐	Biometric access barriers
☐	Light barriers/motion sensors
☒	Manual locking system including key regulation (key book, key issue)
☒	Visitor logging
☒	Careful selection of security staff
☒	Chip cards/transponder locking systems
☒	Video monitoring of access doors
☒	Safety locks
☒	Personnel screening by gatekeeper/reception
☒	Careful selection of cleaning staff
☒	Obligation to wear employee/guest ID cards
☐	Other:

2. DATA ACCESS CONTROL/USER CONTROL

Prevention of the use of automated processing systems by unauthorized persons by means of data transmission equipment (e.g. screensavers with passwords).

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

Specifications for the measures:

☒	Authentication with user name/password (passwords assigned based on the valid password regulations)
☐	Usage of intrusion detection systems
☒	Usage of anti-virus software
☒	Usage of a software firewall
☒	Creation of user profiles
☒	Assignment of user profiles to IT systems
☒	Usage of VPN technology
☒	Encryption of mobile data storage media
☐	Encryption of data storage media in laptops
☐	Usage of central smartphone administration software (e.g. for the external erasure of data)
☐	Other:

3. DATA USAGE CONTROL/DATA STORAGE MEDIA CONTROL/MEMORY CONTROL

Prevention of unauthorized reading, copying, modification or deletion of data carriers (data storage media control), prevention of unauthorized input of personal data as well as unauthorized knowledge, modification and deletion of stored personal data (data storage media control).

Guarantee that the persons authorized to use an automated processing system have access only to the personal data based on their access authorization (e.g. by means of authorization concepts, passwords, regulations governing the resignation and transfer of employees). (data usage control).

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

2. DATA TOEGANGSCONTROLE/GEBRUIKERSCONTROLE

Voorkomen van het gebruik van geautomatiseerde verwerkingssystemen door onbevoegden door middel van gegevensoverdrachtapparatuur (bijv. screensavers met wachtwoorden).

Corporate Manual Wachtwoordregeling (M60.02.01)
Bedrijfsstandaardprocedure voor identificatie en autorisatie van gebruikers van IT-systemen
Corporate Standard CUSTOMER Security Regulation (vervangt M60.02.10)
Corporate Standard Mobile Environment Governance (vervangt M60.05.01)

Specifications for the measures:

☒	Authentication with user name/password (passwords assigned based on the valid password regulations)
☐	Usage of intrusion detection systems
☒	Usage of anti-virus software
☒	Usage of a software firewall
☒	Creation of user profiles
☒	Assignment of user profiles to IT systems
☒	Usage of VPN technology
☒	Encryption of mobile data storage media
☐	Encryption of data storage media in laptops
☐	Usage of central smartphone administration software (e.g. for the external erasure of data)
☐	Other:

3. BEHEER VAN GEGEVENSGEBRUIK/DATAOPSLAG MEDIABEHEER/GEHEUGENBEHEER

Voorkomen van ongeoorloofd lezen, kopiëren, wijzigen of wissen van gegevensdragers (beheer van gegevens-opslagmedia), voorkomen van ongeoorloofde invoer van persoonsgegevens alsmede ongeoorloofde kennisname, wijziging en verwijdering van opgeslagen persoonsgegevens (controle van gegevensopslagmedia).

Garantie dat de personen die geautoriseerd zijn om een geautomatiseerd verwerkingssysteem te gebruiken alleen toegang hebben tot de persoonsgegevens op basis van hun toegangsautorisatie (bijvoorbeeld door middel van autorisatieconcepten, wachtwoorden, regelingen voor het ontslag en overplaatsing van werknemers).
(controle van gegevensgebruik).

Corporate Manual Wachtwoordregeling (M60.02.01)
Bedrijfsstandaardprocedure voor identificatie en autorisatie van gebruikers van IT-systemen
Bedrijfsstandaardclassificatie en controle van informatie
Bedrijfshandleiding Beveiligingsrichtlijnen voor databases - 3.4.6 Gegevensintegriteit

Specifications for the measures:

☒	Roles and authorizations based on a "need to know principle"
☒	Number of administrators reduced to only the "essentials"
☒	Logging of access to applications, in particular the entry, change and erasure of data
☒	Physical erasure of data storage media before reuse
☒	Use of shredders or service providers
☒	Administration of rights by defined system administrators
☒	Password guidelines, incl. password length and changing passwords
☒	Secure storage of data storage media
☒	Proper destruction of data storage media (DIN 32757)
☐	Logging of destruction
☐	Other:

4. TRANSFER CONTROL/TRANSPORTATION CONTROL

Ensuring the confidentiality and integrity of data during the transmission of personal information and the transport of data carriers (e.g. through powerful encryption of data transmissions, closed envelopes for mailings, encrypted storage on data carriers).

Corporate Standard Classification and Control of Information

Specifications for the measures:

☒	Establishment of dedicated lines or VPN tunnels
☒	Encrypted data transmission on the Internet (such as HTTPS, SFTP, etc.)
☒	E-mail encryption (transport encryption)
☒	Documentation of the recipients of data and time frames of planned transmission or agreed erasure deadlines
☐	In case of physical transportation: careful selection of transportation personnel and vehicles
☐	Transmission of data in an anonymized or pseudonymized form
☐	In case of physical transportation: secure containers/packaging
☐	Other:

5. ENTRY CONTROL/TRANSMISSION CONTROL

Ensure subsequent logging and verification of changes (which personal data were entered or modified, when and by whom) within automated processing systems (entry control). Ensure the sufficiently secured and documented transfer (including the secure and adequate transfer methods used) of personal data according to the geographical, physical or electronic transfer to other locations (transfer control).

Continental Information Security Guideline (CISG) – 3.5.10.1 Audit Logging

Specifications for the measures:

☒	Roles and authorizations based on a "need to know principle"
☒	Number of administrators reduced to only the "essentials"
☒	Logging of access to applications, in particular the entry, change and erasure of data
☒	Physical erasure of data storage media before reuse
☒	Use of shredders or service providers
☒	Administration of rights by defined system administrators
☒	Password guidelines, incl. password length and changing passwords
☒	Secure storage of data storage media
☒	Proper destruction of data storage media (DIN 32757)
☐	Logging of destruction
☐	Other:

4. OVERDRACHT CONTROLE/VERVOER CONTROLE

Het waarborgen van de vertrouwelijkheid en integriteit van gegevens tijdens de overdracht van persoonlijke informatie en het transport van gegevensdragers (bijvoorbeeld door krachtige versleuteling van gegevensoverdrachten, gesloten enveloppen voor mailings, versleutelde opslag op gegevensdragers).

Bedrijfsstandaardclassificatie en controle van informatie

Specifications for the measures:

☒	Establishment of dedicated lines or VPN tunnels
☒	Encrypted data transmission on the Internet (such as HTTPS, SFTP, etc.)
☒	E-mail encryption (transport encryption)
☒	Documentation of the recipients of data and time frames of planned transmission or agreed erasure deadlines
☐	In case of physical transportation: careful selection of transportation personnel and vehicles
☐	Transmission of data in an anonymized or pseudonymized form
☐	In case of physical transportation: secure containers/packaging
☐	Other:

5. TOEGANGSCONTROLE / TRANSMISSIECONTROLE

Zorgdragen voor de e logging en verificatie van wijzigingen (welke persoonsgegevens zijn ingevoerd of gewijzigd, wanneer en door wie) binnen geautomatiseerde verwerkingssystemen (invoercontrole). Zorgen voor de voldoende beveiligde en gedocumenteerde overdracht (inclusief de veilige en adequate overdrachtsmethoden die worden gebruikt) van persoonsgegevens volgens de geografische, fysieke of elektronische overdracht naar andere locaties (overdrachtscontrole).

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

Specifications for the measures:

☒	Logging of the entry, change and erasure of data
☒	Traceability of the entry, change and erasure of data through unique user names (not user groups)
☒	Assignment of rights for the entry, change and erasure of data based on an authorization concept
☐	Creating an overview showing which data can be entered, changed and deleted with which applications
☐	Maintaining forms from which data is taken over in automated processing
☐	Other:

Continental Information Security Guideline (CISG) – 3.5.10.1 Auditlogging
Bedrijfsstandaardprocedure voor identificatie en autorisatie van gebruikers van IT-systemen
Bedrijfsstandaardclassificatie en controle van informatie
Bedrijfshandleiding
Beveiligingsrichtlijnen voor databases - 3.4.6 Gegevensintegriteit

Specifications for the measures:

☒	Logging of the entry, change and erasure of data
☒	Traceability of the entry, change and erasure of data through unique user names (not user groups)
☒	Assignment of rights for the entry, change and erasure of data based on an authorization concept
☐	Creating an overview showing which data can be entered, changed and deleted with which applications
☐	Maintaining forms from which data is taken over in automated processing
☐	Other:

6. AVAILABILITY CONTROL/RESTORATION/RELIABILITY/DATA INTEGRITY

Guarantee that systems used can be restored in the event of a malfunction (recoverability). Ensure that all functions of the system are available and that any malfunctions that occur are reported (reliability). Guarantee that stored personal data cannot be damaged by system malfunctions (data integrity). Guarantee that personal data is protected against accidental destruction or loss (availability control), e.g. by implementing suitable backup and disaster recovery concepts.

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

Specifications for the measures:

☒	Uninterruptible Power Supply (UPS)
☒	Devices for monitoring temperature and moisture in server rooms
☒	Fire and smoke detector systems
☐	Alarms for unauthorized access to server rooms
☒	Tests of data restorability
☒	Storing data back-ups in a separate and secure location
☐	In flood zones: server rooms above the high water level
☒	Air conditioning units in server rooms
☐	Protected outlet strips in server rooms
☒	Fire extinguishers in server rooms
☒	Creating a back-up and recovery concept
☐	Creating an emergency plan
☐	Other:

6.BESCHIKBAARHEIDSCONTROLE/HERSTEL/ BETROUWBAARHEID/GEGEVENSINTEGRITEIT

Garanderen dat gebruikte systemen bij een storing hersteld kunnen worden (herstelbaarheid). Zorg ervoor dat alle functies van het systeem beschikbaar zijn en dat eventuele storingen worden gemeld (betrouwbaarheid). Garanderen dat opgeslagen persoonsgegevens niet kunnen worden beschadigd door systeemstoringen (data-integriteit). Garanderen dat persoonsgegevens beschermd zijn tegen onopzettelijke vernietiging of verlies (beschikbaarheidscontrole), b.v. door geschikte back-up- en noodherstelconcepten te implementeren.

Bedrijfshandleiding Backup and Recovery Security Regulation (M60.02.08)

Specifications for the measures:

☒	Uninterruptible Power Supply (UPS)
☒	Devices for monitoring temperature and moisture in server rooms
☒	Fire and smoke detector systems
☐	Alarms for unauthorized access to server rooms
☒	Tests of data restorability
☒	Storing data back-ups in a separate and secure location
☐	In flood zones: server rooms above the high water level
☒	Air conditioning units in server rooms
☐	Protected outlet strips in server rooms
☒	Fire extinguishers in server rooms
☒	Creating a back-up and recovery concept
☐	Creating an emergency plan
☐	Other:

7. SEPARATION CONTROL / SEPARABILITY

Ensuring that data collected for different purposes can be processed separately. (e.g. by logical separation of customer data, special access controls (authorization concept), separation of test and production data.)

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

Specifications for the measures:

☒	Physically separated storing on separate systems or data storage media
☐	Including purpose attributions/data fields in data sets
☒	Establishing database rights
☐	Logical CUSTOMER separation (software-based)
☐	For pseudonymized data: separation of mapping file and storage on a separate, secured IT system
☒	Separation of production and testing systems
☐	Other:

7. SCHEIDINGSCONTROLE/SCHEIDBAARHEID:

Ervoor zorgen dat gegevens die voor verschillende doeleinden zijn verzameld, afzonderlijk kunnen worden verwerkt. (o.a. door logische scheiding van klantgegevens, speciale toegangscontroles (autorisatieconcept), scheiding van test- en productiegegevens.)

Continental Information Security Guideline (CISG) – 3.5.1.4 Scheiding van ontwikkel-, test- en operationele faciliteiten

Specifications for the measures:

☒	Physically separated storing on separate systems or data storage media
☐	Including purpose attributions/data fields in data sets
☒	Establishing database rights
☐	Logical CUSTOMER separation (software-based)
☐	For pseudonymized data: separation of mapping file and storage on a separate, secured IT system
☒	Separation of production and testing systems
☐	Other:

APPENDIX III – SUB-PROCESSORS / INTERNATIONAL TRANSFERS

CONTINENTAL ensures an appropriate level of technical and organizational security measures at the Sub-Processors involved in order to process personal data within an appropriate and secure framework (Adequacy of the Sub-Processor).

If Sub-Processors are involved in the processing of personal data (e.g., hosting, provision of data center space, cloud services, operating software etc.), the implementation of technical and organizational measures by the respective Sub-Processor will be ensured by corresponding data processing agreements. Sub-Processors must - with sufficient warranty - ensure at least the same technical and organizational measures as agreed between the Customer and CONTINENTAL.

To prevent and/or avoid unauthorized access and/or unauthorized attempted access to CONTINENTAL's IT-Systems and storage facilities including data stored there - whether from external or internal or by Sup-Processors - CONTINENTAL has implemented permanent control and monitoring measures for its IT-Systems including access-control / access-monitoring (24/7, 365 days) by implementing state-of-the-art intrusion detection systems / firewalls / access control, etc. If unauthorized access or unauthorized attempted access is detected, it will be automatically terminated without delay. The Service Team of Continental Automotive Technologies GmbH in Europe has the exclusive control over these security systems; access to these systems by Processors or others is excluded.

The following Sub-Processors / Subcontractors are involved by CONTINENTAL:

	APPLICABLE ONLY IN CASE CONTINENTAL AUTOMOTIVE TECHNOLOGIES GMBH IS NOT THE DIRECT CONTRACTING PARTY TO THE CUSTOMER AND IS ACTING AS SUB-PROCESSORS OF <RSOS/NATIONAL DEALERS/PARTNERS> (APPLICABLE FOR ALL COUNTRIES / CUSTOMERS):
☐	**Continental Automotive Technologies GmbH**, Vahrenwalder Straße 9, 30165 Hannover, Germany (Development and Support)

APPENDIX III – SUBVERWERKERS / INTERNATIONAAL DATAVERKEER

CONTINENTAL zorgt voor de juiste technische en organisatorische beveiligingsmaatregelen bij de betrokken Subverwerkers om persoonsgegevens te verwerken binnen een passend en veilig kader (adequaatheid van de Subverwerker).

Als Subverwerkers betrokken zijn bij de verwerking van persoonsgegevens (bijv. hosting, levering van datacenterruimte, clouddiensten, besturingssoftware enz.), wordt de implementatie van technische en organisatorische maatregelen door de respectievelijke Subverwerker verzekerd door overeenkomstige afspraken over gegevensverwerking. Subverwerkers moeten - met voldoende garantie - zorgen voor ten minste dezelfde technische en organisatorische maatregelen als overeengekomen tussen de Klant en CONTINENTAL.

Om ongeoorloofde toegang en/of pogingen tot toegang tot de IT-systemen en opslagfaciliteiten van CONTINENTAL te voorkomen en/of te vermijden, met inbegrip van gegevens die daar zijn opgeslagen - hetzij van externe of interne of door Subverwerkers - heeft CONTINENTAL permanente controle- en bewakingsmaatregelen voor haar IT-systemen geïmplementeerd, waaronder toegangscontrole/ toegangsbewaking (24 uur per dag, 7 dagen per week, 365 dagen per jaar), door state-of-the-art inbraakdetectiesystemen/firewalls/toegangscontrole/etc. te implementeren. Als ongeautoriseerde toegang of een ongeautoriseerde poging tot toegang wordt gedetecteerd, wordt deze automatisch en onmiddellijk beëindigd. Het serviceteam van Continental Automotive Technologies GmbH in Europa heeft de exclusieve controle over deze beveiligingssystemen; toegang tot deze systemen door Processors of anderen is uitgesloten.

De volgende Subverwerkers/Onderaannemers zijn betrokken bij CONTINENTAL:

	ALLEEN VAN TOEPASSING INDIEN CONTINENTAL AUTOMOTIVE TECHNOLOGIES GMBH NIET DE DIRECT VERWERKER IS EN OPGESTELD IS ALS ONDERAANNEMER VAN RSO'S/NATIONALE DISTRIBUTEURS/PARTNERS. (VAN TOEPASSING VOOR ALLE LANDEN / KLANTEN)
☐	**Continental Automotive Technologies GmbH**, Vahrenwalder Straße 9, 30165 Hannover, Germany (Development and Support)

	SUB-PROCESSORS OF CONTINENTAL AUTOMOTIVE TECHNOLOGIES GMBH (APPLICABLE FOR ALL COUNTRIES / CUSTOMERS):
☒	**Com-a-tec GmbH**, Am Krebsgraben 15, 78048 Villingen-Schwenningen, Germany (Support Level 2)
☒	**Continental AG**, Hauptverwaltung, Vahrenwalder Straße 9, 30165 Hannover, Germany. Continental AG is the contract holder regarding the provision of services by the Sub-Processor of Continental AG towards Continental Automotive Technologies GmbH as listed below separately
☒	**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 Compon ents India is a Continental Group Company which provides **Development, Monitoring and support on the services.** **Please note:** Any access by Continental Automotive Components India to (personal) data of VDO Fleet-Customer within the EEA is subject to the Binding Corporate Rules of the Continental Group which ensures an adequate level of data protection in the meaning of Art 45 et seq. GDPR.
☒	**Continental Digital Services France SAS**, 1 avenue Paul Ourliac B.P.13704 31037 Toulouse, France Continental Digital Services France is a Continental Group Company which provides **Development, Monitoring and support on the services.**
☒	**Eviden Germany GmbH,** Otto-Hahn Ring 6, 81739 München (Support and Maintenance)
☒	**Google Ireland Limited,** Gordon House, Barrow Street, Dublin 4, Ireland (Provider of Cloud Services, e.g., Google Cloud Platform)

	SUBVERWERKERS VAN CONTINENTAL AUTOMOTIVE TECHNOLOGIES GMBH (VAN TOEPASSING VOOR ALLE LANDEN/KLANTEN):
☒	**Com-a-tec GmbH**, Am Krebsgraben 15, 78048 Villingen-Schwenningen, Germany (Serviceniveau 2)
☒	**Continental AG** Hoofdkantoor, Vahrenwalder Straße 9, 30165 Hannover, Germany Continental AG is de contracthouder voor de diensten van Subverwerkers t.a.v. Contientnal Automotive technologies GmbH zoals hieronder vermeld.
☒	**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 is een Continental Group Company diensten verleent voor ontwikkeling en het moninotren en ondersteunen van deze diensten. **Please note:** Elk toegang tot van Continental Automotive Components India tot (persoonlijke) data van VDO Fleet-klanten binnen de EEG valt onder de bindende regels van de Continental Group die data voldoende protectie borgt zoals is beschreven in Art 45 et seq. GDPR.
☒	**Continental Digital Services France SAS**, 1 avenue Paul Ourliac B.P.13704 31037 Toulouse, France Continental Digital Services France is a Continental Group Company voor Ontwikkeling, Monitoren en support levert voor deze dienst.
☒	**Eviden Germany GmbH,** Otto-Hahn Ring 6, 81739 München (Ondersteuning en onderhoud)
☒	**Google Ireland Limited,** Gordon House, Barrow Street, Dublin 4, Ireland (Leverancier van cloudservices, bijv. Google Cloud Platform) **Let op:** Google zal worden gebruikt als "Subverwerker" voor de levering van clouddiensten. In dit verband heeft CONTINENTAL ervoor gezorgd dat de gegevens afkomstig uit de Europese Economische Ruimte (EER) alleen binnen de EER worden verwerkt, vrijgesteld als anders

	Please note: Google will be used as "Sub-Processor" for the provision of cloud services. In this respect, CONTINENTAL has ensured that the data originated within the European Economic Area (EEA) will only be processed within the EEA, exempt as otherwise agreed with the CUSTOMER. In addition, and as fallback, the Standard-Contractual-Clauses of the EU-Commission are in place (as provided by the Commissions' Implementing Decision (EU) 2021/914 of 04.06.2021) as also the new adequacy decision of the EU Commission for data processing in the USA of 10.07.2023 apply. In addition, Continental has implemented specific technical security measures as described above to prevent unauthorized access to data, especially from outside the EEA.		overeengekomen met de KLANT. Aanvullend, en als uitwijkmogelijkheid, zijn de Standaard Contractuele Clausules van de EU-Commissie van kracht (zoals bepaald in het Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 04.06.2021) en is ook het nieuwe adequaatheidsbesluit van de Europese Commissie voor gegevensverwerking in de VS van 10.07.2023 van toepassing. Daarnaast heeft Continental specifieke technische beveiligingsmaatregelen geïmplementeerd zoals hierboven beschreven om ongeoorloofde toegang tot gegevens te voorkomen, met name van buiten de EER.
☒	**kernel concepts GmbH**, Hauptstraße 16, 57074 Siegen (Provider of kernel services, improvement, maintenance etc., data will be processed within the EEA only)	☒	**kernel concepts GmbH**, Hauptstraße 16, 57074 Siegen (Leverancier van kerneldiensten, verbetering, onderhoud enz., data wordt alleen binnen de EER verwerkt)
	SUBPROCESSOR OF CONTINENTAL AUTOMOTIVE TRADING FRANCE SAS (ONLY APPLICABLE FOR FRANCE / FRENCH CUSTOMERS):		**SUBVERWERKERS VAN CONTINENTAL AUTOMOTIVE TRADING FRANCE SAS (ALLEEN VAN TOEPASSING VOOR FRANKRIJK/FRANSE KLANTEN):**
☒	**IMA TECHNOLOGIES**, 31 Route de Gachet 44300 Nantes, France (Support Hotline)	☒	**IMA TECHNOLOGIES**, 31 Route de Gachet 44300 Nantes, France (Support Hotline)
	SUBPROCESSOR OF CONTINENTAL AG (APPLICABLE FOR ALL COUNTRIES / CUSTOMERS):		**SUBVERWERKERS VAN CONTINENTAL AG (VAN TOEPASSING VOOR ALLE LANDEN / KLANTEN)**
☒	**SYZYGY Deutschland GmbH**, Im Atzelnest 3, 61352 Bad Homburg, Germany (Hosting-Services)	☒	**SYZYGY Deutschland GmbH,** Im Atzelnest 3, 61352 Bad Homburg, Germany (Hosting-services)
☒	**MongoDB Limited, Ireland,** 3 Shelbourne Buildings, Ballsbridge, Dublin 4, Ireland (Provider of Cloud Services; the cloud services are restricted to the EEA.)	☒	**MongoDB Limited, Ireland,** 3 Shelbourne Buildings, Ballsbridge, Dublin 4, Ireland (Leverancier van clouddiensten; de clouddiensten zijn beperkt tot de EER)
	SUB-PROCESSORS OF CONTINENTAL DIGITAL SERVICES FRANCE SAS (APPLICABLE FOR ALL COUNTRIES / CUSTOMERS):		**SUB-PROCESSORS VAN CONTINENTAL DIGITAL SERVICES FRANCE SAS (VAN TOEPASSING VOOR ALLE LANDEN / KLANTEN):**
☒	**Clearblade Inc**., 1701 Directors BLVD STE 250, Austin, TX 78744, USA	☒	**Clearblade Inc.**, 1701 Directors BLVD STE 250, Austin, TX 78744, USA

	(Solution for managing telematic device connections, Support / Maintenance) **Please note:** Continental has ensured that the services and data originated within the EEA will only be processed on servers within the EEA. In addition, and as a fallback, the standard contractual clauses of the EU Commission (see Commission Implementing Decision (EU) 2021/914 of 04.06.2021) have been agreed with Clearblade. In addition, Continental has implemented specific technical security measures as described above to prevent unauthorized access to data, especially from outside the EEA.
☒	**DataDog Inc.,** New York Times Bldg, 620 8th Ave 45th Floor, New York, MA, USA (Support & Availability Services) **Please note:** Data Dog only processes pseudonymized, aggregated data; in addition, and as fallback the Standard-Contractual-Clauses of the EU-Commission are in place (as provided by the Commissions' Implementing Decision (EU) 2021/914 of 04.06.2021) as also the new adequacy decision of the EU Commission for data processing in the USA of 10.07.2023 apply. In addition, Continental has implemented specific technical security measures as described above to prevent unauthorized access to data, especially from outside the EEA.
☒	**Frisbii Germany GMBH (Billwerk),** Mainzer Landstrasse 51, 60329 Frankfurt a. M. (Provider of Billing Solutions) **Please note:** Continental has ensured that the services and data originated within the EEA will only be processed on servers within EEA.
☒	**OKTA Inc.**, 100 First Street, 6th Floor, San Francisco, CA 94105, USA (Service Provider Customer Identity & Access Management (CIAM)) **Please note:** Continental has ensured that the services and data originated within the EEA will only be processed on servers within the EEA. In addition, and as a fallback, the standard contractual clauses of the EU Commission (see Commission Implementing Decision (EU)

	(Oplossing voor het beheren van telematica-apparaatverbindingen,Ondersteuning/onderhoud) **Let op:** Continental heeft ervoor gezorgd dat de diensten en gegevens die afkomstig zijn uit de EER alleen worden verwerkt op servers binnen de EER. Aanvullend, en als uitwijkmogelijkheid, zijn de modelcontractbepalingen van de Europese Commissie (zie Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 04.06.2021) overeengekomen met Clearblade, aangezien ook het nieuwe adequaatheidsbesluit van de Europese Commissie voor gegevensverwerking in de VS van 10.07.2023 van toepassing is. Daarnaast heeft Continental specifieke technische beveiligingsmaatregelen geïmplementeerd zoals hierboven beschreven om ongeoorloofde toegang tot gegevens te voorkomen, met name van buiten de EER.
☒	**DataDog Inc.,** New York Times Bldg, 620 8th Ave 45th Floor, New York, MA, USA (Ondersteunings- & beschilbaarheidsservices) **Let op:** Data Dog verwerkt alleen gepseudonimiseerde, geaggregeerde gegevens; aanvullend, en als uitwijkmogelijkheid, zijn de Standaard-Contractuele-Clausules van de EU-Commissie van kracht (zoals bepaald in het Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 04.06.2021) en is ook het nieuwe adequaatheidsbesluit van de Europese Commissie voor gegevensverwerking in de VS van 10.07.2023 van toepassing. Daarnaast heeft Continental specifieke technische beveiligingsmaatregelen geïmplementeerd zoals hierboven beschreven om ongeoorloofde toegang tot gegevens te voorkomen, met name van buiten de EER.
☒	**Frisbii Germany GMBH (Billwerk),** Mainzer Landstrasse 51, 60329 Frankfurt a. M. (Aanbieder van factuuroplossingen) **Let op:** Continental heeft ervoor gezorgd dat de diensten en gegevens afkomstig uit de EER alleen worden verwerkt op servers binnen de EER.
☒	**OKTA Inc.**, 100 First Street, 6th Floor, San Francisco, CA 94105, USA (Service Provider voor Customer Identity & Access Management (CIAM)) **Let op:** Continental heeft ervoor gezorgd dat de diensten en gegevens die afkomstig zijn uit de EER alleen worden verwerkt op servers binnen de EER.

	2021/914 of 04.06.2021) have been agreed with Okta as also the new adequacy decision of the EU Commission for data processing in the USA of 10.07.2023 apply. In addition, Continental has implemented specific technical security measures as described above to prevent unauthorized access to data, especially from outside the EEA.
☒	**pendo.io Inc.,** 150 Fayetteville St., Raleigh, NC 27601, USA; European Representative (Art. 27 GDPR): DP-Dock GmbH, Ballindamm 39, 20095 Hamburg (Support & Development Services) **Please note:** pendo.io only processes pseudonymized, aggregated data. The data will only be processed and stored within the EEA. In addition, and as fallback, the Standard-Contractual-Clauses of the EU-Commission are in place (as provided by the Commissions' Implementing Decision (EU) 2021/914 of 04.06.2021) as also the new adequacy decision of the EU Commission for data processing in the USA of 10.07.2023 apply. In addition, Continental has implemented specific technical security measures as described above to prevent unauthorized access to data, especially from outside the EEA.

	Aanvullend, en als uitwijkmogelijkheid, zijn de modelcontractbepalingen van de Europese Commissie (zie Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 04.06.2021) overeengekomen met Okta, aangezien ook het nieuwe adequaatheidsbesluit van de Europese Commissie voor gegevensverwerking in de VS van 10.07.2023 van toepassing is. Daarnaast heeft Continental specifieke technische beveiligingsmaatregelen geïmplementeerd zoals hierboven beschreven om ongeoorloofde toegang tot gegevens te voorkomen, met name van buiten de EER.
☒	**pendo.io Inc.,** 150 Fayetteville St., Raleigh, NC 27601, USA; European Representative (Art. 27 GDPR): DP-Dock GmbH, Ballindamm 39, 20095 Hamburg (Ondersteunings- en ontwikkelingsservices) **Let op:** pendo.io verwerkt alleen gepseudonimiseerde, geaggregeerde gegevens. De gegevens worden alleen binnen de EER verwerkt en opgeslagen. Aanvullend, en als uitwijkmogelijkheid, zijn de Standaard Contractuele Clausules van de EU-Commissie van kracht (zoals bepaald in het Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 04.06.2021) en is ook het nieuwe adequaatheidsbesluit van de Europese Commissie voor gegevensverwerking in de VS van 10.07.2023 van toepassing. Daarnaast heeft Continental specifieke technische beveiligingsmaatregelen geïmplementeerd zoals hierboven beschreven om ongeoorloofde toegang tot gegevens te voorkomen, met name van buiten de EER.

General information: Your rights as part of the European General Data Protection Regulation remain unchanged. CONTINENTAL furthermore confirms that your data will be stored in data centers in the European Union. CONTINENTAL uses highest security standards (e.g., ISO/DIN/https/encryption) and protects personal data during transmission and storage.

Algemene informatie: Uw rechten als onderdeel van de Europese Algemene Verordening Gegevensbescherming blijven ongewijzigd. CONTINENTAL bevestigt bovendien dat uw gegevens worden opgeslagen in datacenters in de Europese Unie. CONTINENTAL hanteert de hoogste beveiligingsnormen (bijv. ISO/DIN/https/encryptie) en beschermt persoonsgegevens tijdens verzending en opslag.

Geautoriseerde VDO Fleet partners:
Smart Tacho Solutions B.V. Tankval 30, 2408 ZC Alphen aan den Rijn, Nederland (Customer Support Hotline) **Opmerking:** toegang tot klantgegevens voor ondersteuning wordt alleen verleend aan de geautoriseerde partner, die in het contract is vastgelegd.
CKO Parts B.V. Franklinstraat 17, 6003 DK Weert, Nederland (Customer Support Hotline) **Opmerking:** toegang tot klantgegevens voor ondersteuning wordt alleen verleend aan de geautoriseerde partner, die in het contract is vastgelegd.
Tachograph Telematic Solutions B.V. Lijster 9, 1722 DC Zuid-Scharwoude, Nederland (Customer Support Hotline) **Opmerking:** toegang tot klantgegevens voor ondersteuning wordt alleen verleend aan de geautoriseerde partner, die in het contract is vastgelegd.
SA Rauwers Controle Rue François-Joseph Navez 78/86, 1000 Brussel, België (Customer Support Hotline) **Opmerking:** toegang tot klantgegevens voor ondersteuning wordt alleen verleend aan de geautoriseerde partner, die in het contract is vastgelegd.
Phelect SPRL Rue des Trois Entites 15, 4890 Thimister-Clermont, België (Customer Support Hotline) **Opmerking:** toegang tot klantgegevens voor ondersteuning wordt alleen verleend aan de geautoriseerde partner, die in het contract is vastgelegd.

* *