VERWERKERSOVEREENKOMST (DPA) VOOR VDO FLEET ONLINE (BIJLAGE C)

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:

SECTIE I

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) 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.

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.

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.

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.

Sectie II
VERPLICHTINGEN VAN DE PARTIJEN

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.

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

b) De verwerker informeert de verwerkingsverantwoordelijke direct indien, volgens de opinie van de verwerker, instructies gegeven worden door de verwerker met vermeende inbreuk op verordening (EU) 2015/799 / Verordening (EU) 2018/1725 of nationale of vakbondsregels met betrekking tot data privacy.

7.2. Doel beperking

Verwerker zal de persoonsgegevens alleen verwerken voor de specifieke doeleinden van de 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) De verwerker past ten minste de in bijlage II genoemde technische en organisatorische maatregelen toe om de beveiliging van de persoonsgegevens te waarborgen. Dit omvat de bescherming van de gegevens tegen een inbreuk op de beveiliging die leidt tot accidentele of onwettige vernietiging, verlies, wijziging, niet-geautoriseerde bekendmaking of toegang tot de gegevens (inbreuk in verband met persoonsgegevens). Bij de beoordeling van het passende beveiligingsniveau houden de partijen rekening met de stand van de techniek, de uitvoeringskosten, de aard, de omvang, de context en de 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.

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.

e) 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. 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.

b) 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 laterewijzigingen 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 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.

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;

ii. 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.

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.

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

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 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

Annex I: Details van de verwerking

Annex II: Technische en organisatorische maatregelen ter bescherming van persoonsgegevens onder de werking van de DPA, geïmplementeerd door CONTINENTAL.

Annex III: Sub- en dataverwerkers / internationale data-overdracht

VDO FLEET ONLINE
(CONTINENTAL AFTERMARKET & SERVICES GMBH, VERSION 1.6, 26.07.2023
ANNEX C (I)/ BIJLAGE C (I)

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 VDO FLEET ONLINE-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. CATEGORIEËN VAN BETROKKENEN:

- ☒ Klanten
- ☐ Bezoekers
- ☐ Beursdeelnemers
- ☒ Gebuikers van diensten
- ☒ Deelnemers aan communicatie
- ☒ Abonnees
- ☐ Geïnteresseerden
- ☐ Leverancier en/of service provider (individuele contacten bij deze partijen)
- ☒ Werknemers
- ☐ Sollicitanten
- ☐ Voormalige werknemers
- ☐ Leerlingen, stagiairs
- ☐ Familieleden van werknemers
- ☐ Consultants
- ☒ Verkoopvertegenwoordigers
- ☐ Aandeelhouders/organen
- ☒ Zakelijke contactpersonen
- ☐ Leveranciers en/of service providers
- ☒ Zakenpartners
- ☒ Anderen, a.u.b. specificeren: degenen die in dienst zijn bij klanten, bijv. chauffeurs en gebruikers van VDO Fleet-diensten

4. PERSOONSGEGEVENS

Algemeen/privë contactgegevens

- ☒ Namen persoonlijke profielen
- ☐ Foto
- ☒ Privé adresgegevens
- ☒ Geboortedatum
- ☒ Gegevens ID-kaart (paspoort, rijbewijs)
- ☐ Andere, a.u.b. specificeren: _____

Contractgegevens

- ☒ Afrekenings- en betalingsgegevens
- ☒ Bank- of creditcard-gegevens
- ☒ Financiële draagkracht/kredietwaardigheid
- ☒ Contract geschiedenis
- ☐ Andere, a.u.b. specificeren _____

VDO FLEET ONLINE
(CONTINENTAL AFTERMARKET & SERVICES GMBH, VERSION 1.6, 26.07.2023
ANNEX C (I)/ BIJLAGE C (I)

Zakelijke gegevens

☒ Persoonlijke gegevens
☐ Functie- en arbeidsgegevens
☒ Prestatiemanagement
☐ Kwalificatie en opleidingsgegevens
☒ Gegevens sociale zekerheid
☒ Afwezigheid van werk
☒ Andere, a.u.b. specificeren

- toegangsgegevens van de klant en zijn operators/gebruikers
- bestuurdersgegevens (bijv. naam, adres (bedrijfs- of privé-adres), geslacht, verjaardag, rijbewijsnummer, kaartnummer enz.)
- voertuiggegevens en voertuigprofielen
- communicatiegegevens (bv. telefoon, e-mail)
- bewegingsgegevens, GPS-gegevens
- activiteiten en profiel van bestuurders, waaronder rij- en rusttijden overeenkomstig aanhangsel 1B van Verordening (EU) nr. 561/2006, Verordening (EU) nr. 2020/1054, Verordening (EG) nr. 1360/2002, Verordening nr. 165/2014 en Uitvoeringsverordening (EU) nr. 2016/799.
- gegevens voor het gebruik van de dienst door gebruikers downloadgegevens voor de bestuurderskaart en de tachograaf

Gegevens over diensten en IT-gebruik

☐ Apparaat-identificatiegegevens
☒ Gebruiks- en aanslutingsgegevens
☐ Beeld-/videogegevens
☒ Telecommunicatiegegevens/berichtinhoud
☐ Audio-/spraakgegevens
☐ Identificatiegegevens
☒ Toegangsgegevens
☐ Machtiging
☐ Metagegevens
☐ Andere, a.u.b. specificeren:_____

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.

Speciale categorieën van persoonsgegevens

☐ Ras of etniciteit
☐ Religieuze of filosofische overtuiging
☐ Lichamelijke of geestelijke gezondheid
☐ Politieke opvattingen
☐ Biometrische gegevens
☐ Genetische gegevens
☐ Lidmaatschap van een vakbond
☐ Seksueel leven
☐ Strafbare feiten, veroordelingen of vonnissen
☐ Andere, a.u.b. specificeren:_____

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.

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

Specificaties voor de maatregelen:

☒	Alarmsysteem
☒	Automatisch toegangscontrolesysteem
☐	Afsluitsysteem met codeslot
☐	Biometrische toegangsbarrières
☐	Lichtbarrières/bewegingssensoren
☒	Handmatig afsluitsysteem inclusief sleutelregeling (sleutelboek, sleuteluitgifte)
☒	Registratie van bezoekers
☒	Zorgvuldige selectie van beveiligingspersoneel
☒	Chipkaarten/transponder-sluitsystemen
☒	Videobewaking van toegangsdeuren
☒	Veiligheidssloten
☒	Personeelscontrole door portier/receptie
☒	Zorgvuldige selectie van schoonmaakpersoneel
☒	Verplichting om ID-kaarten te dragen voor werknemers/gasten
☐	Andere:

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)

Specificaties voor de maatregelen:

☒	Authenticatie met gebruikersnaam/wachtwoord (wachtwoorden toegekend op basis van de geldige wachtwoordvoorschriften)
☐	Gebruik van inbraakdetectiesystemen
☒	Gebruik van antivirussoftware
☒	Gebruik van een firewall
☒	Aanmaken van gebruikersprofielen
☒	Toewijzing van gebruikersprofielen aan IT-systemen
☒	Gebruik van VPN-technologie
☒	Encryptie van mobiele opslagmedia
☐	Encryptie van opslagmedia in laptops
☐	Gebruik van centrale software voor smartphonebeheer (bv. voor het extern wissen van gegevens)
☐	Andere:

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

Specificaties voor de maatregelen:

☒	Rollen en bevoegdheden op basis van een "need to know"-beginsel
☒	Aantal beheerders teruggebracht tot alleen de "essentiële"
☒	Vastlegging van de toegang tot toepassingen, met name het invoeren, wijzigen en wissen van gegevens
☒	Fysiek wissen van gegevensopslagmedia vóór hergebruik
☒	Gebruik van shredders of dienstverleners
☒	Beheer van rechten door gedefinieerde systeembeheerders
☒	Richtlijnen voor wachtwoorden, inclusief de lengte van wachtwoorden en het wijzigen van wachtwoorden
☒	Veilige opslag van gegevensdragers
☒	Juiste vernietiging van gegevensdragers (DIN 32757)
☐	Registratie van vernietiging
☐	Andere:

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.

Specificaties voor de maatregelen:

☒	Totstandbrenging van speciale lijnen of VPN-tunnels
☒	Gecodeerde gegevenstransmissie op het internet (zoals HTTPS, SFTP, enz.)
☒	E-mailversleuteling (transportversleuteling)
☒	Documentatie van de ontvangers van gegevens en termijnen voor geplande overdracht of overeengekomen verwijderingstermijnen
☐	In geval van fysiek vervoer: zorgvuldige selectie van vervoerspersoneel en voertuigen
☐	Overdracht van gegevens in geanonimiseerde of gepseudonimiseerde vorm
☐	In geval van fysiek vervoer: veilige containers/verpakking
☐	Andere:

5. TOEGANGSCONTROLE / TRANSMISSIECONTROLE
Zorgdragen voor de 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).

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

Specificatie van de maatregelen:

☒	Vastlegging van het invoeren, wijzigen en wissen van gegevens
☒	Traceerbaarheid van het invoeren, wijzigen en wissen van gegevens via unieke gebruikersnamen (geen gebruikersgroepen)
☒	Toekenning van rechten voor het invoeren, wijzigen en verwijderen van gegevens op basis van een autorisatieplanning
☐	Het maken van een overzicht waaruit blijkt welke gegevens met welke toepassingen kunnen worden ingevoerd, gewijzigd en verwijderd
☐	Bijhouden van formulieren waaruit gegevens worden overgenomen in geautomatiseerde verwerking
☐	Andere:

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)

Specificaties voor de maatregelen:

☒	Ononderbroken stroomvoorziening (UPS)
☒	Apparaten voor de bewaking van temperatuur en vochtigheid in serverruimten
☒	Brand- en rookdetectiesystemen
☐	Alarmen voor ongeoorloofde toegang tot serverruimten
☒	Testen van de herstelbaarheid van gegevens
☒	Opslag van gegevensback-ups op een afzonderlijke en veilige locatie
☐	In overstromingsgebieden: serverruimten boven het hoogwaterpeil
☒	Airconditioning-units in serverruimtes
☐	Beveiligde contactdozen in serverruimten
☒	Brandblussers in serverruimtes
☒	Een back-up- en herstelplan opstellen
☐	Een noodplan opstellen
☐	Andere:

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

Specificaties voor de maatregelen:

☒	Fysiek gescheiden opslag op afzonderlijke systemen of gegevensdragers
☐	Specificaties voor de maatregelen:
☒	Vaststelling van databaserechten
☐	Logische scheiding van KLANTEN (op basis van software)
☐	Voor gepseudonimiseerde gegevens: scheiding van mappingbestand en opslag op een afzonderlijk, beveiligd IT-systeem
☒	Scheiding van productie- en testsystemen
☐	Andere:

BIJLAGE III – ONDERAANNEMERS / SUBVERWERKERS / INTERNATIONALE DATAVERKEER

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

Als Sub-processors 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. Sub-processors 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 Sub-processors - 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 Sub-processors/Onderaannemers zijn betrokken bij CONTINENTAL:

	SUB-PROCESSORS VAN TOEPASSING VOOR ALLE LANDEN/KLANTEN:
☒	**Eviden Germany GmbH,** Otto-Hahn Ring 6, 81739 München (Ondersteuning en onderhoud)
☒	**Clearblade Inc.**, 1701 Directors BLVD STE 250, Austin, TX 78744, USA (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.
☒	**Com-a-tec GmbH**, Am Krebsgraben 15, 78048 Villingen-Schwenningen, Germany (Serviceniveau 2)
☒	**Continental Automotive Technologies GmbH en gelieerde groepsmaatschappijen**, Vahrenwalder Straße 9, 30165 Hannover, Germany (Ontwikkeling en ondersteuning)
☒	**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.
☒	**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 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 (Leverancier van kerneldiensten, verbetering, onderhoud enz., data wordt alleen binnen de EER verwerkt)
☒	**MongoDB Limited, Ireland,** 3 Shelbourne Buildings, Ballsbridge, Dublin 4, Ireland (Leverancier van clouddiensten; de clouddiensten zijn beperkt tot 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. 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.
☒	**SYZYGY Deutschland GmbH**, Im Atzelnest 3, 61352 Bad Homburg, Germany (Hosting-services)
☒	**Thales**, 31 Place des Corolles, CS 20001 – 92098 Paris La Défense, France (Leverancier van van encryptiesleutels voor hosting in een key management systeem – KMS)
☒	**Zonar Systems, Inc.**, 18200 Cascade Ave S, Seattle, WA 98188, USA, een volledige dochteronderneming van Continental Group. Zonar Systems biedt ondersteuning, onderhoud en ontwikkelingsservices voor de TIS-Web-Services van CONTINENTAL. **Let op:** Elke toegang van Zonar Systems tot (persoons-)gegevens van VDO Fleet-klanten binnen de EER is onderworpen aan de bindende bedrijfsregels van de Continental Group die een adequaat niveau van gegevensbescherming in de zin van artikel 45 e.v. AVG waarborgen, net zoals 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.
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.
	A1 Automotive B.V. Tweelingenlaan 102, 7324 BP Apeldoorn, Nederland (Customer Support Hotline) **Opmerking:** toegang tot klantgegevens voor ondersteuning wordt alleen verleend aan de geautoriseerde partner, die in het contract is vastgelegd.
	Info-Instruments B.V. Hazeldonk 6521, 4836 LD Breda, 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.

Algemene informatie: Uw rechten zoals beschreven in de European General Data Protection Regulation blijven ongewijzigd. CONTINENTAL bevestigd dat KLANT data bewaard wordt in datacenters gelegen binnen de Europese Unie onder de strengste veiligheidseisen (e.g. ISO/DIN/https/encryption) en beveiligd persoonlijke data tijdens dataverkeer en opslag.

* * *