

## Overeenkomst inzake de verwerking van gegevens (hierna te noemen: Verwerkersovereenkomst) voor VDO-Fleet Services

Deze Verwerkersovereenkomst regelt de wettelijke verplichtingen van de Partijen inzake de bescherming van persoonsgegevens bij de verwerking daarvan in het kader van het VDO FLEET Services Contract (hierna 'Hoofdcontract' genoemd). De Verwerkersovereenkomst is van toepassing op alle activiteiten die verband houden met het Hoofdcontract waarbij medewerkers van de Opdrachtnemer en/of door Opdrachtnemer ingeschakelde derden toegang hebben tot door de Klant verstrekte persoonsgegevens.

### 1. VOORWERP EN DUUR VAN DE OVEREENGEKOMEN VERWERKING

Opdrachtnemer verzamelt, verwerkt of gebruikt persoonsgegevens uitsluitend namens en in overeenstemming met de instructies van Klant. Opdrachtnemer is verantwoordelijk voor het naleven van de wettelijke bepalingen inzake de bescherming van persoonsgegevens.

#### 1.1 Doeleinden van de overeengekomen gegevensverwerking:

De doeleinden ten behoeve waarvan gegevens worden verwerking vloeien voort uit het door Partijen afgesloten Hoofdcontract en, indien beschikbaar, de toepasselijke service contracten (service descriptions). Dit houdt met name in dat de Opdrachtnemer de volgende taken zal uitvoeren:

De omvang van de verwerking wordt gedetailleerd beschreven in de service contracten (Service descriptions) van Continental Automotive Trading Nederland B.V. voor de VDO FLEET Services en de functionele productoverzichten.

#### 1.2 Duur van de verwerking:

De duur van de overeengekomen verwerking is gelijk aan de duur van het Hoofdcontract en/of eventuele individuele contracten of orders op basis van een raamovereenkomst.

#### 1.3 Beëindiging zonder kennisgeving:

Klant kan deze Verwerkersovereenkomst, alsmede de Hoofd-overeenkomst, zonder opzegtermijn met onmiddellijke ingang beëindigen, indien de Opdrachtnemer verwijtbaar inbreuk maakt op wettelijke bepalingen inzake de bescherming van gegevens en/of de verplichtingen uit hoofde van de Verwerkersovereenkomst.

### 2. Inhoud van de te verwerken data:

Opdrachtnemer zal alleen persoons-gegevens verzamelen, verwerken of gebruiken in het kader van de door Partijen overeengekomen verwerking en volgens de instructies van Klant (zie ook art. 8 ).

#### 2.1 Omvang, aard en doel van de overeengekomen gegevensverwerking:

De omvang, aard en het doel van het verzamelen, verwerken en/of gebruiken van persoonsgegevens wordt in detail ontleend aan het Hoofdcontract. Dit houdt met name in dat de volgende procedures voor gegevensverwerking worden gevolgd:

Continental Automotive Trading Nederland B.V is uitsluitend gerechtigd persoonsgegevens te verzamelen, te verwerken en te gebruiken in overeenstemming met de VDO FLEET Services en de instructies van de Klant (zie ook art 8).

Meer informatie over de omvang, de aard en het doel van het verzamelen, verwerken en/of gebruiken van persoonsgegevens is te vinden in de Algemene Voorwaarden behorend bij het Hoofdcontract en de functionele productoverzichten.

#### 2.2 Soort gegevens

In het bijzonder zijn de navolgende soorten/categorieën persoonsgegevens onderwerp van verzameling, verwerking of gebruik:

- X Persoonsgegevens;
- X Communicatiegegevens (zoals telefoon, e-mail)
- X Contractgegevens (contractuele relatie, product of contractuele belangen)
- X Voorgeschiedenis van de Klant
- X Facturatie en betalingsgegevens
- X Bankgegevens (rekeningnummer, bankcode of IBAN)
- Planning- en controlegegevens
- X Gegevens verkregen van derden, zoals van kredietinstellingen of uit openbare registers
- Speciale categorieën gegevens
- X Overige:...
  - toegangsggegevens van de Klant en zijn uitvoerders / gebruikers
  - bestuurdersgegevens
  - voertuiggegevens en voertuigprofielen
  - communicatiegegevens (bijv. telefoon, e-mail)
  - verplaatsingsgegevens, GPS-gegevens
  - activiteiten van bestuurders en inzetprofiel, met inbegrip van rij- en rusttijden overeenkomstig aanhangsel 1B van Verordening EU 561/2006
  - gegevens voor het gebruik van de dienst door gebruikers
  - downloadgegevens voor de bestuurderskaart en tachograaf

- 2.3 Betrokkenen:
- Van onder meer de volgende categorieën personen worden persoonsgegevens verwerkt:
  - X Klanten
  - Medewerkers
  - Leveranciers
  - X Contactpersonen
- X Overige: ...
- Klanten
  - Personen in dienst van de Klant, zijnde bestuurders en gebruikers van VDO FLEET Services.
- 2.4 Technische / organisatorische maatregelen:  
Voor zover niet anders is bepaald in de Service contracten of het Hoofdcontract, worden de door Opdrachtnemer getroffen technische en organisatorische maatregelen beschreven in bijlage 1 bij deze Verwerkersovereenkomst. De technische en organisatorische maatregelen zijn onderhevig aan technologische proces- en verdere ontwikkelingen. Opdrachtnemer is daarom gerechtigd om adequate alternatieve maatregelen te implementeren. Het beveiligingsniveau van de toegepaste maatregelen mag in elk geval niet in het gedrang komen. Belangrijke wijzigingen moeten door Opdrachtnemer worden gedocumenteerd
3. **Rechten van de betrokkenen – rectificatie, recht op beperking van verwerking en het recht op vergetelheid**
- 3.1 Klant dient betrokken te zijn bij de waarborging van de rechten van de betrokkene en moet zorgen voor de naleving van de overeenkomstige wettelijke verplichtingen van Klant, in het bijzonder met betrekking tot meldingen aan betrokkene(n), het verstrekken van informatie aan betrokkene(n) en het recht op rectificatie, wissen en/of beperking van de verwerking van persoonsgegevens.
- 3.2 Opdrachtnemer mag de persoons-gegevens alleen rectificeren, wissen of de verwerking ervan beperken overeenkomstig de instructies van Klant. In geval een betrokkene rechtstreeks contact opneemt met de Opdrachtnemer om zijn gegevens te laten rectificeren of wissen, moet de Opdrachtnemer dit verzoek onmiddellijk doorsturen naar Klant.
- 3.3 Indien Klant wettelijk verplicht is om informatie met betrekking tot het verzamelen, verwerken of gebruiken van persoonsgegevens aan natuurlijke personen (betrokkenen) te verstrekken, moet de Opdrachtnemer de Klant ondersteunen bij het verstrekken van deze informatie indien
- a) Klant de Opdrachtnemers verzoekt om dit schriftelijk te doen.
  - b) Klant de kosten die de Opdrachtnemer voor deze ondersteunende diensten maakt.
4. **Inspecties en overige verantwoordelijkheden van Opdrachtnemer:**
- 4.1 Opdrachtnemer is verder verantwoordelijk voor het naleven van de volgende verplichtingen:  
Bescherming van de geheimhouding: Alle personen die toegang hebben tot persoonlijke informatie van de Klant in het kader van hun contractuele plichten moeten tot geheimhouding worden verplicht.
- 4.2 Implementatie en naleving van alle nodige technische en organisatorische maatregelen (zie ook artikel 0).
4. **Inspecties en overige verantwoordelijkheden van Opdrachtnemer:**
- 4.1 Opdrachtnemer is verder verantwoordelijk voor het naleven van de volgende verplichtingen:  
Bescherming van de geheimhouding: Alle personen die toegang hebben tot persoonlijke informatie van de Klant in het kader van hun contractuele plichten moeten tot geheimhouding worden verplicht.
- 4.2 Implementatie en naleving van alle nodige technische en organisatorische maatregelen (zie ook artikel 0).
- 4.3 De mogelijk om op verzoek van de Klant de genomen technische en organisatorische maatregelen te verifiëren.  
Opdrachtnemer kan actuele verklaringen, verslagen of uittreksels uit verslagen van onafhankelijke instanties (zoals auditors, inspecteurs, functionarissen voor de gegevens-bescherming, IT-beveiligingsafdeling-en, gegevensbeschermingsauditors en kwaliteitsauditors) of een passende certificering van een IT-beveiligings- of gegevensbeschermingsaudit voor-leggen (bijv. conform de BSI Basic Protection).
- 4.4 Controles door middel van regelmatige beoordelingen uitgevoerd door de Opdrachtnemer, inzake de uitvoering of nakoming van de overeengekomen gegevensverwerking, in het bijzonder de naleving van en eventuele noodzakelijke wijzigingen aan voor-schriften en maatregelen inzake de overeengekomen gegevensverwerking. Melding aan de Klant van tekortkomingen en/of onregelmatigheden die bij de beoordeling werden ontdekt.
- 4.5 Schriftelijke aanstelling - indien wettelijk vereist - van een functionaris voor gegevensbescherming (DPO). De Klant krijgt de beschikking over contactgegevens om rechtstreeks contact te kunnen opnemen met de DPO.
- 4.6 Verstrekking van de volledige schriftelijke documentatie inzake het verzamelen, verwerken of gebruiken van persoonsgegevens, op basis waarvan de Klant te allen tijde de rechtmatigheid van de gegevensverwerking kan aantonen.

- 4.7 Verstreking van informatie en gegevens die nodig zijn voor de Klant om verwerkingsactiviteiten te kunnen registreren; dergelijke informatie mag alleen worden verstrekt op verzoek van Klant en alleen met betrekking tot de gegevens die door Opdrachtnemer in het kader van deze Verwerkersovereenkomst zijn verwerkt.
- Onderaannemers**
- 5.1 Indien onderaannemers zijn betrokken bij de verwerking of het gebruik van persoonsgegevens van de Klant, moet er worden voldaan aan de volgende voorwaarden:
- Opdrachtnemer moet de onderaannemer zorgvuldig selecteren en voor het sluiten van de overeenkomst controleren of deze in staat is om te voldoen aan overeenkomsten gesloten tussen Partijen.
  - Het inhuren van onderaannemers is in het principe alleen toegestaan na schriftelijke toestemming van de Klant.
  - Opdrachtnemer moet de overeenkomsten met de onderaannemer(s) zodanig opstellen dat er wordt voldaan aan de bepalingen inzake gegevensbescherming die van toepassing zijn op de contractuele relatie tussen Partijen.
- 5.2 Indien de Klant reeds toestemming heeft verleend voor het gebruik van onderaannemers, staan deze vermeld in **bijlage 1** bij deze Verwerkersovereenkomst. Elke latere betrokkenheid van onderaannemers met toestemming van de Klant dient te worden gedocumenteerd.
- 5. Onderaannemers**
- 5.1 Indien onderaannemers zijn betrokken bij de verwerking of het gebruik van persoonsgegevens van de Klant, moet er worden voldaan aan de volgende voorwaarden:
- Opdrachtnemer moet de onderaannemer zorgvuldig selecteren en voor het sluiten van de overeenkomst controleren of deze in staat is om te voldoen aan overeenkomsten gesloten tussen Partijen.
  - Het inhuren van onderaannemers is in het principe alleen toegestaan na schriftelijke toestemming van de Klant.
  - Opdrachtnemer moet de overeenkomsten met de onderaannemer(s) zodanig opstellen dat er wordt voldaan aan de bepalingen inzake gegevensbescherming die van toepassing zijn op de contractuele relatie tussen Partijen.
- 5.2 Indien de Klant reeds toestemming heeft verleend voor het gebruik van onderaannemers, staan deze vermeld in **bijlage 1** bij deze Verwerkersovereenkomst. Elke latere betrokkenheid van onderaannemers met toestemming van de Klant dient te worden gedocumenteerd.
- 5.3 Diensten die de Opdrachtnemer als bijkomende diensten uitvoert om de Opdrachtnemer te ondersteunen bij de uitvoering van de overeengekomen verwerking van gegevens, mogen niet worden beschouwd als onderaannemingsrelaties in de zin van deze overeenkomst. Deze diensten omvatten bijv. telecommunicatiediensten, onderhouds- en gebruikersdiensten, schoonmaakdiensten, audits of verwijdering van media voor gegevensopslag. Opdrachtnemer is echter wel verplicht om passende en rechtsgeldige overeenkomsten te sluiten en om controlemaatregelen te treffen om de bescherming en beveiliging van gegevens van de Klant te waarborgen, mede met betrekking bijkomende diensten die zijn ingekocht bij derden.
- 6. Zeggenschapsrechten van de Klant**
- 6.1 Opdrachtnemer gaat ermee akkoord dat de Klant te allen tijde het recht heeft om -na schriftelijke kennisgeving- de naleving van de voorschriften inzake de bescherming van gegevens en de bepalingen van deze Verwerkersovereenkomst door Opdrachtnemer te controleren, in het bijzonder door informatie in te winnen en opgeslagen gegevens en verwerkingsprogramma's te inspecteren. Klant heeft het recht de naleving van de Verwerkers-overeenkomst door Opdrachtnemer steekproefsgewijs te controleren.
- 6.2 Opdrachtnemer is verplicht om de Klant op zijn verzoek alle informatie te verschaffen die nodig is ter naleving van zijn verplichtingen met betrekking tot overeengekomen verwerking en om de relevante attesten ter beschikking te stellen.
- 6.3 Ten behoeve van de inspecties door de Klant voor en tijdens de overeengekomen verwerking, zorgt de Opdrachtnemer ervoor dat hij de Klant voldoende bewijs van de naleving van de overeengekomen technische en organisatorische maatregelen kan overleggen. In dat verband voorziet Opdrachtnemer de Klant van het bewijs dat de technische en organisatorische maatregelen die dit tot doel hebben zijn geïmplementeerd (zie artikel 0). Het bewijs kan ook verstrekt worden door het overleggen van actuele verklaringen, verslagen of uittreksels van verslagen afkomstig van onafhankelijke instanties (zoals auditors, inspecteurs, functionarissen voor de bescherming van persoonsgegevens, IT-beveiligingsafdelingen, gegevensbeschermings- auditors en kwaliteitsauditors) of via relevante certificering van een IT-beveiliging- of gegevensbeschermingsaudit (bijv. conform de BSI Basic Protection).
- 7. Kennisgeving van een data inbreuk**
- 7.1 Opdrachtnemer stelt Klant op de hoogte van elk geval van en inbreuk in verband met persoonsgegevens waarvoor de Opdrachtnemer, zijn medewerkers of onderaannemers verantwoordelijk zijn.
- 7. Kennisgeving van een data inbreuk**
- 7.1 Opdrachtnemer stelt Klant op de hoogte van elk geval van en inbreuk in verband met persoonsgegevens waarvoor de Opdrachtnemer, zijn medewerkers of onderaannemers verantwoordelijk zijn.

- 7.2 Indien het verlies, de onrechtmatige overdracht of de openbaarmaking van persoonsgegevens mogelijk een risico's met zich meebrengen voor de rechten en vrijheden van natuurlijke personen (betrokkenen), kunnen er meldverplichtingen jegens regulerende instantie of de betrokkene zelf gelden. Daarom moet Klant onmiddellijk op de hoogte worden gebracht van dergelijke gevallen, ongeacht de oorzaak daarvan. Dit geldt ook in geval van ernstige verstoringen van het bedrijfsproces, de verdenking van overtreding van de wetgeving inzake de bescherming van persoonsgegevens of andere onregelmatigheden bij de verwerking van persoonsgegevens van Klant.
- 7.3 Opdrachtnemer neemt in overleg met de Klant passende maatregelen om gegevens te beveiligen en eventuele negatieve gevolgen voor de betrokkenen te beperken. Indien er voor de Klant in geval van inbreuk in verband met persoonsgegevens een meldingsplicht bestaat bij toezichhouders, dient de Opdrachtnemer de Klant daarbij te ondersteunen.
- 8. Bevoegdheid van de Klant om richtlijnen uit te vaardigen**
- 8.1 Persoonsgegevens mogen uitsluitend verwerkt worden in het kader van de gesloten overeenkomsten en in overeenstemming met de instructies van Klant. Klant behoudt zich het recht voor om richtlijnen uit te vaardigen met betrekking tot de aard, de omvang en het proces van de verwerking, en om – d.m.v. individuele instructies- verdere concrete details te verstrekken. Wijzigingen in de doeleinden van de verwerking en procedures moeten in onderling overleg worden overeengekomen en gedocumenteerd. De Opdrachtnemer mag alleen informatie verstrekken aan derde partijen of betrokkenen met de voorafgaande schriftelijke toestemming van de Klant.
- 8.2 Mondelinge instructies moeten onmiddellijk schriftelijk door de Klant worden gemeld (bijv. e-mail). Opdrachtnemer gebruikt de gegevens voor geen enkel ander doel. Zonder medeweten van de opdrachtgever worden geen kopieën of duplicaten gemaakt. Dit geldt niet voor reservekopieën die nodig zijn ter waarborging van correcte gegevensverwerking en voor gegevens die nodig zijn om te voldoen aan de wettelijke archiveringsplichten.
- 8.3 Opdrachtnemer informeert de Klant onmiddellijk als hij vermoedt dat instructies van de Klant een inbreuk zijn op de voorschriften voor de bescherming van gegevens. Opdrachtnemer heeft het recht om de uitvoering van de betreffende instructie op te schorten totdat deze bevestigd of gewijzigd is door een door de Klant aangewezen verantwoordelijke persoon.
- 9. Openbaarmaking, wissen van gegevens / teruggeven van media voor gegevensopslag**
- 9.1 Opdrachtnemer is verplicht om op verzoek van de Klant of bij beëindiging van de overeengekomen gegevensverwerking, doch niet later dan aan het einde van de contractuele relatie met Klant, alle documenten die hij heeft gekregen, alle verkregen dataopslag- media, alle voorbereide verwerkings- en gebruikresultaten en alle gearchiveerde gegevens die verband houden met de contractuele relatie of die het resultaat zijn van de overeengekomen gegevensverwerking aan de Klant of aan een door Klant aangewezen derde partij terug te geven. Deze verplichting geldt ook voor kopieën en/of reproducties van media voor gegevensopslag en/of gearchiveerde gegevens. Opdrachtnemer heeft geen retentierecht inzake deze gegevens.
- 9.2 Na het teruggeven van de gegevens overeenkomstig de bepaling van artikel 9.1, of indien de Klant afziet van teruggave, moeten gegevens die zich nog op de gegevensdragers van de Opdrachtnemer bevinden –na toestemming van de Klant- worden vernietigd of gewist conform de wetgeving ter bescherming van persoonsgegevens. Opdrachtnemer moet op verzoek van de Klant aan de hand van passende documentatie en/of relevante waarborgen bewijzen dat het wissen is voltooid.
- De Klant mag niet eisen dat de bewaarde gegevens door de Opdrachtnemer worden gewist, indien de Opdrachtnemer wettelijk verplicht is om deze data te archiveren; deze gegevens mogen voorts alleen worden verwerkt door de Opdrachtnemer. Dergelijke gegevens mogen alleen worden verwerkt in plaats van gewist, indien dit wettelijk is toegestaan (bijv. op grond van lokale of nationale uitvoeringsvoorschriften inzake gegevensbescherming), in het bijzonder wanneer wissen niet mogelijk is door het specifieke type archivering of indien het met onredelijk veel werk gepaard zou gaan.
- 9.3 Documentatie die dient om te bewijzen dat de gegevensverwerking verloopt conform deze verplichtingen uit hoofde van de Verwerkersovereenkomst en de relevante wetgeving, moet door de Opdrachtnemer worden gearchiveerd voor het einde van de Verwerkersovereenkomst; conform de toepasselijke archiverings-voorwaarden.
- Aan het einde van deze Verwerkers-overeenkomst kan de betreffende documentatie aan de Klant worden overgedragen zodat zij ook in de gelegenheid is om deze taak te vervullen.
- 9.4 De voorschriften van de artikelen 9.1 en 9.2 zijn overeenkomstig van toepassing op test- en restmateriaal.
- 10. Verplichtingen van de Klant**
- 10.1 Klant is verantwoordelijk voor de naleving van de wettelijke bepalingen ter bescherming van gegevens, in het bijzonder voor de rechtmatigheid van de overdracht van gegevens aan de Opdrachtnemer.

- 
- 10.2 Klant verstrekt de Opdrachtnemer onmiddellijk de volledige informatie wanneer zij bij de beoordeling van verwerkingsresultaten tekortkomingen of onregelmatigheden ontdekt met betrekking tot de bepalingen van de wetgeving inzake de bescherming van gegevens.
- 10.3 Klant houdt een administratie bij van de verwerkingsactiviteiten.
- 10.4 Klant moet ervoor zorgen dat er schriftelijke toestemming wordt verkregen van zijn medewerkers voor het verzamelen en verwerken van hun persoonsgegevens met het oog op het gebruik van de VDO Fleet Services, doch voor zover deze toestemming wettelijk verplicht is gesteld.
11. **Aansprakelijkheid**
- 11.1 De in deze Verwerkersovereenkomst vermelde verplichtingen ter bescherming van gegevens betreffen belangrijke contractuele verplichtingen voor de Opdrachtnemer (fundamentele verplichtingen) van het Hoofdcontract gesloten met Klant. In dat opzicht moet deze Verwerkersovereenkomst worden beschouwd als een aanvulling op het Hoofdcontract.
- 11.2 Opdrachtnemer is jegens Klant aansprakelijk voor schade die Klant lijdt als gevolg van een verwijtbare schending van regels inzake gegevensbeschermings en/of de verplichtingen uit de Verwerkersovereenkomst door Opdrachtnemer; met inachtneming van aansprakelijkheidsregels zoals vermeld in het Hoofdcontract.
12. **Hoofdcontract**
- 12.1 Verhouding tot het Hoofdcontract, overige verplichtingen en bepalingen.  
Voor zover in de Verwerkersovereenkomst niet anders is bepaald, hebben de bepalingen van deze Verwerkersovereenkomst inclusief bijlagen voorrang op het Hoofdcontract en dienen deze als aanvulling daarop.
- 12.2 Indien de door Opdrachtnemer opgeslagen gegevens van de Klant in gevaar worden gebracht door beslaglegging, inbeslagneming, faillissement- of schikkings-procedure of door andere gebeurtenissen of maatregelen die door derden zijn geïnitieerd, dient de Opdrachtnemer de Klant daarvan onmiddellijk op de hoogte te brengen. De Opdrachtnemer brengt alle verantwoordelijke partijen ter zake onmiddellijk van op de hoogte dat de Klant het exclusieve eigendom heeft van de gegevens, overgedragen media voor gegevensopslag, documenten, etc.
- 12.3 Voor wijzigingen en/of aanpassingen van deze Verwerkersovereenkomst is een schriftelijke akte vereist. Dit geldt ook voor zover er afstand wordt gedaan van het schriftelijke vormvereiste.
- 12.4 Met betrekking tot het toepasselijke recht en de forumkeuze zijn de toepasselijke bepalingen van het Hoofdcontract van toepassing.

### Technische en organisatorische maatregelen voor de overeengekomen gegevensverwerking

De maatregelen zijn vastgelegd in de goedgekeurde 'Binding Corporate Rules of the Continental Corporation' en worden toegepast op basis van de bestaande IT-veiligheidsrichtlijnen.

Specifieke maatregelen met betrekking tot deze Verwerkersovereenkomst vindt u in de onderstaande punten.

Met de respectieve onderaannemers zijn de adequate maatregelen voor gegevensverwerking in een afzonderlijk contract vastgelegd.

#### Fysieke toegangscontrole

Waarborging van de toelating/toegang tot verwerkingssystemen waarmee de verwerking wordt uitgevoerd tegen onbevoegde personen (bijv. door middel van fysieke eigendomsbescherming: omheining, portier, slagboom voor personeel, draaihek, deur met kaartlezer, camerabewaking, organisatorische eigendomsbescherming, reglement betreffende toegangsrechten, toegangsregistratie)

De volgende technische en organisatorische maatregelen werden door de Opdrachtnemer getroffen voor het verzamelen, verwerken of gebruiken van de persoonsgegevens beschreven in de Verwerkersovereenkomst :

<input checked="" type="checkbox"/>	Alarmsysteem
<input checked="" type="checkbox"/>	Automatisch toegangscontrolesysteem
<input type="checkbox"/>	Vergrendelingsstelsel met codevergrendeling
<input type="checkbox"/>	Biometrische toegangsslagbomen
<input type="checkbox"/>	Lichtbarrières/bewegingssensoren
<input checked="" type="checkbox"/>	Handmatig vergrendelingsstelsel inclusief sleutelregulatie (sleutelboek, sleuteluitgifte)
<input checked="" type="checkbox"/>	Registratie van bezoekers
<input checked="" type="checkbox"/>	Zorgvuldige selectie van beveiligingsmedewerkers
<input checked="" type="checkbox"/>	Chipkaarten/transpondervergrendelingsstelsels
<input checked="" type="checkbox"/>	Videobewaking van toegangsdeuren
<input checked="" type="checkbox"/>	Veiligheidssloten
<input checked="" type="checkbox"/>	Screening van personeel door portier/receptie
<input checked="" type="checkbox"/>	Zorgvuldige selectie van schoonmaakpersoneel
<input checked="" type="checkbox"/>	Verplichting tot het dragen van werknemer/gast ID-kaarten
<input type="checkbox"/>	Diversen:

#### Gegevenstoegangs-/gebruikerscontrole

Voorkomen dat derden gebruikmaken van automatische verwerkingssystemen met apparatuur voor gegevensoverdracht (authenticatie met gebruikersnaam en wachtwoord).

De volgende technische en organisatorische maatregelen werden door de Opdrachtnemer getroffen voor het verzamelen, verwerken of gebruiken van de persoonsgegevens beschreven in de Verwerkersovereenkomst :

<input checked="" type="checkbox"/>	Authenticatie met gebruikersnaam/wachtwoord (wachtwoorden toegekend op basis van de geldige wachtwoordvoorschriften)
<input type="checkbox"/>	Gebruik van inbraakdetectiesystemen
<input checked="" type="checkbox"/>	Gebruik van antivirussoftware
<input checked="" type="checkbox"/>	Gebruik van een software-firewall
<input checked="" type="checkbox"/>	Aanmaken van gebruikersprofielen
<input checked="" type="checkbox"/>	Toewijzing van gebruikersprofielen aan IT-systemen
<input checked="" type="checkbox"/>	Gebruik van VPN-technologie
<input checked="" type="checkbox"/>	Codering van mobiele media voor gegevensopslag
<input type="checkbox"/>	Codering van media voor gegevensopslag op laptops
<input type="checkbox"/>	Gebruik van centrale software voor het beheer van smartphones (bijv. voor het extern wissen van gegevens)
<input type="checkbox"/>	Diversen:



### Controle van het gegevensgebruik/controle van de gegevensopslagmedia/geheugen- controle

Voorkomen van onbevoegd lezen, kopiëren, wijzigen of wissen van media voor gegevensopslag (controle van media voor gegevensopslag), voorkomen van onbevoegde invoer van persoonlijke informatie en onbevoegde toegang daartoe, wijzigen en verwijderen van opgeslagen persoonlijke informatie (geheugencontrole). Ervoor zorgen dat de partijen die bevoegd zijn om een geautomatiseerd verwerkingssysteem te gebruiken, alleen toegang hebben tot de persoonlijke informatie die past bij hun toegangsbevoegdheid (bijv. door middel van bevoegdheidsconcepten, wachtwoorden, voorschriften voor het verlaten van het bedrijf en voor het verhuizen van medewerkers naar andere afdelingen.) (controle op het gebruik van gegevens).

De volgende technische en organisatorische maatregelen werden door de Opdrachtnemer getroffen voor het verzamelen, verwerken of gebruiken van de persoonsgegevens beschreven in de Verwerkersovereenkomst :

<input checked="" type="checkbox"/>	Rollen en bevoegdheden gebaseerd op een 'need-to-know'-principe
<input checked="" type="checkbox"/>	Aantal beheerders beperkt tot alleen de "essentiële"
<input checked="" type="checkbox"/>	Registratie van toegang tot applicaties, in het bijzonder het invoeren, wijzigen of wissen van gegevens
<input checked="" type="checkbox"/>	Fysiek wissen van gegevensdragers voor hergebruik
<input checked="" type="checkbox"/>	Gebruik van papierversnipperaars of dienstverleners
<input checked="" type="checkbox"/>	Beheer van rechten door aangewezen systeembeheerders
<input checked="" type="checkbox"/>	Richtlijnen voor wachtwoorden, incl. wachtwoordlengte en het wijzigen van wachtwoorden
<input checked="" type="checkbox"/>	Veilige opslag van media voor gegevensopslag
<input checked="" type="checkbox"/>	Correcte vernietiging van media voor gegevensopslag (DIN 32757)
<input type="checkbox"/>	Registratie van vernietiging
<input type="checkbox"/>	Diversen:

### Overdrachtscontrole/transportcontrole

Ervoor zorgen dat de vertrouwelijkheid en integriteit van gegevens worden beschermd tijdens de overdracht van persoonlijke informatie en het vervoer van media voor gegevensopslag (bijv. door krachtige codering van gegevensoverdrachten, gesloten enveloppen die in mailings worden gebruikt, gecodeerde opslag op media voor gegevensopslag).

De volgende technische en organisatorische maatregelen werden door de Opdrachtnemer getroffen voor het verzamelen, verwerken of gebruiken van de persoonsgegevens beschreven in de Verwerkersovereenkomst :

<input checked="" type="checkbox"/>	Aanleg van speciale lijnen of VPN-tunnels
<input checked="" type="checkbox"/>	Gecodeerde gegevensoverdracht via internet (zoals HTTPS, SFTP, enz.)
<input type="checkbox"/>	E-mail-codering
<input checked="" type="checkbox"/>	Documentatie van de ontvangers van gegevens en tijdschema's voor de geplande overdracht of overeengekomen deadlines voor het wissen van gegevens
<input type="checkbox"/>	In geval van fysiek transport: zorgvuldige selectie van transportpersoneel en voertuigen
<input type="checkbox"/>	Overdracht van gegevens in geanonimiseerde of gepseudonimiseerde vorm
<input type="checkbox"/>	In geval van fysiek transport: veilige containers/verpakking
<input type="checkbox"/>	Diversen:

### Toegangscontrole/overdrachtscontrole

Ervoor zorgen dat achteraf kan worden nagegaan en vastgesteld welke persoonsgegevens op welk moment en door wie ingevoerd of gewijzigd werden in geautomatiseerde verwerkingssystemen bijvoorbeeld via registratie (toegangscontrole). Ervoor zorgen dat, afhankelijk van het systeem, kan worden nagegaan en vastgesteld aan welke kantoren/locaties persoonlijke informatie is verzonden of verstrekt met behulp van apparatuur voor gegevensoverdracht, of naar welke kantoren/locaties deze zouden kunnen worden verzonden (controle op de overdracht).

De volgende technische en organisatorische maatregelen werden door de Opdrachtnemer getroffen voor het verzamelen, verwerken of gebruiken van de persoonsgegevens beschreven in de Verwerkersovereenkomst :

<input checked="" type="checkbox"/>	Registratie van invoer, wijzigen en wissen van gegevens
<input checked="" type="checkbox"/>	Traceerbaarheid van het invoeren, wijzigen en wissen van gegevens via unieke gebruikersnamen (geen gebruikersgroepen)
<input checked="" type="checkbox"/>	Toewijzing van rechten voor het invoeren, wijzigen en wissen van gegevens op basis van een bevoegdheidsconcept
<input type="checkbox"/>	Maken van een overzicht van welke gegevens met welke applicaties kunnen worden ingevoerd, gewijzigd en verwijderd
<input type="checkbox"/>	Bewaren van formulieren waaruit gegevens worden overgenomen voor geautomatiseerde verwerking
<input type="checkbox"/>	Diversen:

### Beschikbaarheidscontrole herstel- betrouwbaarheid/integriteit van gegevens

Ervoor zorgen dat gebruikte systemen kunnen worden hersteld in geval van een storing (herstelbaarheid). Ervoor zorgen dat alle systeemfuncties beschikbaar zijn en dat eventuele storingen worden gemeld (betrouwbaarheid). Ervoor zorgen dat opgeslagen persoonlijke informatie niet kan worden beschadigd door systeemstoringen (gegevensintegriteit). Ervoor zorgen dat persoonsgegevens zijn beschermd tegen abusievelijke vernietiging of verlies (beschikbaarheidscontrole), bijv. door de toepassing van passende back-up- en noodherstelconcepten.

De volgende technische en organisatorische maatregelen werden door de Opdrachtnemer getroffen voor het verzamelen, verwerken of gebruiken van de persoonsgegevens beschreven in de Verwerkersovereenkomst :

<input checked="" type="checkbox"/>	Onderbrekingsvrije voeding (UPS)
<input checked="" type="checkbox"/>	Apparaten voor temperatuur- en vochtbewaking in serverruimten
<input checked="" type="checkbox"/>	Brand- en rookdetectiesystemen
<input type="checkbox"/>	Alarmen voor onbevoegde toegang tot serverruimten
<input checked="" type="checkbox"/>	Tests voor herstelbaarheid van gegevens
<input checked="" type="checkbox"/>	Het opslaan van back-ups van gegevens op een aparte en veilige locatie
<input type="checkbox"/>	In overstromingsgebieden: serverruimten boven het hoge waterniveau
<input checked="" type="checkbox"/>	Airconditioning in serverruimten
<input type="checkbox"/>	Beschermde verdeelstekkers in serverruimten
<input checked="" type="checkbox"/>	Brandblusapparaten in serverruimten
<input checked="" type="checkbox"/>	Opstellen van een back-up- en herstelconcept
<input type="checkbox"/>	Opstellen van een noodplan
<input type="checkbox"/>	Diversen:

### Scheidingscontrole/scheidbaarheid

Ervoor zorgen dat gegevens die werden verzameld voor verschillende doelen afzonderlijk kunnen worden verwerkt (bijvoorbeeld door logische scheiding van klantgegevens, gespecialiseerde toegangscontroles (bevoegdheidsconcept), scheiding van test- en productiegegevens).

De volgende technische en organisatorische maatregelen werden door de Opdrachtnemer getroffen voor het verzamelen, verwerken of gebruiken van de persoonsgegevens beschreven in de Verwerkersovereenkomst :

<input checked="" type="checkbox"/>	Fysiek gescheiden opslag op afzonderlijke systemen of media voor gegevensopslag
<input type="checkbox"/>	Opnemen van doeleigenschappen/gegevensvelden in gegevensverzamelingen
<input checked="" type="checkbox"/>	Invoeren van databankrechten
<input type="checkbox"/>	Logische klantscheiding (softwarematig)
<input type="checkbox"/>	Voor gepseudonimiseerde gegevens: scheiding van mapping-bestand en opslag op een afzonderlijk, beveiligd IT-systeem
<input checked="" type="checkbox"/>	Scheiding van productie- en testsystemen
<input type="checkbox"/>	Diversen:



**ONDERAANNEMERS / SUBVERWERKERS / INTERNATIONALE 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 onderaannemers zijn betrokken door CONTINENTAL bij de VDO FLEET DIENSTEN:

<b>Subverwerkers van toepassing voor alle landen/klanten:</b>	
<input checked="" type="checkbox"/>	<b>Eviden Germany GmbH</b> , Otto-Hahn Ring 6, 81739 München (Ondersteuning en onderhoud)
<input checked="" type="checkbox"/>	<b>Clearblade Inc.</b> , 1701 Directors BLVD STE 250, Austin, TX 78744, USA (Oplossing voor het beheren van telematica-apparaatverbindingen, Ondersteuning/onderhoud)  <b>Let op:</b> 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.
<input checked="" type="checkbox"/>	<b>Com-a-tec GmbH</b> , Am Krebsgraben 15, 78048 Villingen-Schwenningen, Germany (Serviceniveau 2)
<input checked="" type="checkbox"/>	<b>Continental Automotive Technologies GmbH and affiliated group companies</b> , Vahrenwalder Straße 9, 30165 Hannover, Germany (Ontwikkeling en ondersteuning)
<input checked="" type="checkbox"/>	<b>DataDog Inc.</b> , New York Times Bldg, 620 8 <sup>th</sup> Ave 45 <sup>th</sup> Floor, New York, MA, USA (Ondersteunings- & beschikbaarheidsservices)  <b>Let op:</b> 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.
<input checked="" type="checkbox"/>	<b>Google Ireland Limited</b> , Gordon House, Barrow Street, Dublin 4, Ireland (Leverancier van clouddiensten, bijv. Google Cloud Platform)  <b>Let op:</b> 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.
<input checked="" type="checkbox"/>	<b>kernel concepts GmbH</b> , Hauptstraße 16, 57074 Siegen (Leverancier van kerneldiensten, verbetering, onderhoud enz., data wordt alleen binnen de EER verwerkt)
<input checked="" type="checkbox"/>	<b>MongoDB Limited, Ireland</b> , 3 Shelbourne Buildings, Ballsbridge, Dublin 4, Ireland (Leverancier van clouddiensten; de clouddiensten zijn beperkt tot de EER)
<input checked="" type="checkbox"/>	<b>OKTA Inc.</b> , 100 First Street, 6th Floor, San Francisco, CA 94105, USA (Service Provider voor Customer Identity & Access Management (CIAM))

	<p><b>Let op:</b> 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.</p>
<input checked="" type="checkbox"/>	<p><b>pendo.io Inc.</b>, 150 Fayetteville St., Raleigh, NC 27601, USA;          European Representative (Art. 27 GDPR): DP-Dock GmbH, Ballindamm 39, 20095 Hamburg          (Ondersteunings- en ontwikkelingservices)</p> <p><b>Let op:</b> 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.</p>
<input checked="" type="checkbox"/>	<p><b>SYZYGY Deutschland GmbH</b>, Im Atzelnest 3, 61352 Bad Homburg, Germany          (Hosting-services)</p>
<input checked="" type="checkbox"/>	<p><b>Thales</b>, 31 Place des Corolles, CS 20001 – 92098 Paris La Défense, France          (Leverancier van van encryptiesleutels voor hosting in een key management systeem – KMS)</p>
<input checked="" type="checkbox"/>	<p><b>Alleen van toepassing voor Frankrijk / Franse eindgebruikers</b>  <b>IMA TECHNOLOGIES</b>, 31 Route de Gachet 44300 Nantes, France (Support Hotline)</p>
<input checked="" type="checkbox"/>	<p><b>PAY.NL</b>, Kopersteden 10, 7547 TK Enschede, The Netherlands. Het verzorgen van de automatische incasso</p>
<input checked="" type="checkbox"/>	<p><b>ONDERTEKENEN.NL</b>          Prinsessenhof Amalia, Zijlweg 148A, 2015 BJ Haarlem. Het digitaal ondertekenen van het contract volgens Europese richtlijnen</p>
	<p><b>Algemene informatie:</b> 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</p>