Opdrachtverwerkingsovereenkomst (conform art. 28 AVG)

tussen

de **gebruiker** (zoals gedefinieerd in de hoofdovereenkomst)

(hierna "**opdrachtgever**" genoemd)

en

TB Digital Services GmbH, Oskar-Schlemmer-Str. 19 - 21, 80807 München, Duitsland

(hierna "**opdrachtnemer**" genoemd)
(de opdrachtgever en de opdrachtnemer worden hierna elk een "**partij**" genoemd en samen de "**partijen**").

Inleiding

(A) Deze opdrachtverwerkingsovereenkomst (hierna "**overeenkomst**") is van toepassing op alle activiteiten waarbij de opdrachtnemer in aanraking komt met persoonsgegevens (zoals hieronder gedefinieerd in punt 1.5) van de opdrachtgever, van derde aanbieders of van andere betrokkenen in verband met de in punt 2 beschreven activiteit uit de Algemene Voorwaarden voor het gebruik van het platform en evt. daaronder afgesloten afzonderlijke overeenkomsten voor andere diensten (hierna "**hoofdovereenkomst**")**.**

(B) Volgens deze overeenkomst treedt de opdrachtgever op als verantwoordelijke en de opdrachtnemer als opdrachtverwerker in het kader van een opdrachtverwerking als bedoeld in art. 28 AVG (zoals hieronder gedefinieerd).

De partijen komen daarom het volgende overeen:

1 Definities en interpretatie

1.1 "**Europees recht**" is het toepasselijke recht van de Europese Unie, de toepasselijke wetten van de huidige lidstaten van de Europese Unie en de toepasselijke wetten van elke staat die hierna een lidstaat van de Europese Unie wordt.

1.2 "**Europees recht inzake gegevensbescherming**" is het toepasselijke recht van de Europese Unie voor de verwerking van persoonsgegevens (in het bijzonder de AVG), de toepasselijke wetten van de huidige lidstaten van de Europese Unie voor de verwerking van persoonsgegevens (in het bijzonder het BDSG in de versie die van toepassing is) en de toepasselijke wetten voor de verwerking van persoonsgegevens van elke staat die hierna een lidstaat van de Europese Unie wordt.

1.3 "**AVG**" is de "VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming)".

1.4 "**BDSG**" is de Duitse wet inzake gegevensbescherming (Bundesdatenschutzgesetz).

1.5 "**Persoonsgegevens**" heeft de betekenis zoals gedefinieerd in het BDSG/in de AVG.

2 Onderwerp van de gegevensverwerking / plichten van de opdrachtgever

2.1 Deze overeenkomst regelt de verplichtingen van de partijen in verband met de verwerking van persoonsgegevens van de opdrachtgever door de opdrachtnemer in het kader van de in Bijlage 1 genoemde hoofdovereenkomst.

2.2 Onderwerp en duur van de verwerking, aard en doel van de verwerking, het soort persoonsgegevens, de categorieën van betrokken personen en de rechten en plichten van de verantwoordelijke zijn neergelegd in Bijlage 1 van deze overeenkomst en in de prestatiebeschrijving van de hoofdovereenkomst.

2.3 De opdrachtgever blijft in het kader van de AVG verantwoordelijk en waarborgt de toelaatbaarheid van de verwerking van de persoonsgegevens van de betrokken personen (chauffeur en evt. andere personen). Dienaangaande komt de opdrachtgever in het bijzonder zijn uitgebreide informatieplicht na en zorgt ervoor dat voor de verwerking van de persoonsgegevens een rechtsgrondslag in het kader van de wetgeving inzake gegevensbescherming aanwezig is (bijv. afsluiting van een ondernemingsovereenkomst, beperking van de verwerking ten behoeve van het dienstverband).

3 Verplichtingen van de opdrachtnemer

3.1 De opdrachtnemer verwerkt persoonsgegevens van de opdrachtgever uitsluitend voor de in Bijlage 1 genoemde doeleinden en in het kader van de hoofdovereenkomst, alsmede in de opdracht en volgens de in Bijlage 1 gedocumenteerde instructies van de opdrachtgever; de opdrachtnemer verwerkt de persoonsgegevens in verband met deze overeenkomst voor geen andere doeleinden. De buiten het kader van deze overeenkomst vallende verwerking voor eigen doeleinden conform punt 8.3.4 van de hoofdovereenkomst blijft hierdoor onverlet. Kopieën of duplicaten van persoonsgegevens worden niet zonder medeweten van de opdrachtgever gemaakt. Hiervan uitgezonderd zijn back-upkopieën voor zover deze noodzakelijk zijn voor een correcte gegevensverwerking, evenals gegevens die nodig zijn voor de naleving van de wettelijke bewaarplicht.

3.2 Na afloop van de levering van de verwerkingsdiensten moet de opdrachtnemer alle persoonsgegevens van de opdrachtgever, naar diens keuze, overhandigen aan de opdrachtgever en/of deze zelf in overeenstemming met de eisen van de gegevensbescherming wissen, voor zover de wettelijke

bewaartermijnen dit niet in de weg staan en voor zover de opdrachtnemer deze niet voor eigen doeleinden buiten deze overeenkomst conform punt 8.3.4 van de hoofdovereenkomst verwerkt. Hetzelfde geldt voor test- en afvalmateriaal. Het volledig wissen van de gegevens resp. de overdracht ervan aan de opdrachtgever moet aan deze opdrachtgever op diens verzoek schriftelijk met vermelding van de datum worden bevestigd.

3.3 Voor zover bij de prestatieomvang inbegrepen, ondersteunt de opdrachtnemer de opdrachtgever bij het vervullen van de rechten van betrokkenen (inzage, rectificatie, bezwaar, wissing) overeenkomstig de instructie van de opdrachtgever.

3.4 De opdrachtnemer bevestigt dat hij – voor zover wettelijk vereist – een functionaris voor de gegevensbescherming heeft aangesteld (vgl. § 38 BDSG/art. 37 AVG).

3.5 De opdrachtnemer is verplicht de opdrachtgever onmiddellijk in kennis te stellen van de uitkomst van controles door de toezichthouders op de gegevensbescherming, voor zover deze betrekking hebben op de verwerking van de gegevens van de opdrachtgever. De opdrachtnemer zal eventueel vastgestelde bezwaren binnen een redelijke termijn verhelpen en dit mededelen aan de opdrachtgever.

3.6 De verwerking van de gegevens door de opdrachtnemer en de door de opdrachtgever goedgekeurde onderaannemers vindt uitsluitend plaats binnen het grondgebied van de Bondsrepubliek Duitsland, in een lidstaat van de Europese Unie of in een andere staat die partij is bij de Overeenkomst betreffende de Europese Economische Ruimte. Elke verplaatsing naar een ander land (hierna "**derde land**") moet vooraf uitdrukkelijk worden goedgekeurd door de opdrachtgever en mag bovendien alleen plaatsvinden wanneer aan de bijzondere voorwaarden voor gegevensexporten naar derde landen is voldaan (vgl. art. 40 e.v. AVG). Hiervoor zijn de gegevens uit Bijlage 1 vereist en moeten indien nodig extra (contractuele) documenten worden bijgevoegd.

3.7 De opdrachtnemer moet de medewerkers die betrokken zijn bij de uitvoering van de werkzaamheden vertrouwd maken met de voor hen relevante bepalingen van de gegevensbescherming en hen verplichten tot geheimhouding van de gegevens (vgl. art. 28 AVG lid 3 b)), en er door gepaste stappen voor zorgen dat deze medewerkers persoonsgegevens alleen verwerken volgens de instructies van de opdrachtgever.

3.8 De opdrachtnemer controleert tijdens de totale looptijd van de overeenkomst regelmatig de naleving van de in deze overeenkomst neergelegde voorschriften inzake gegevensbescherming, evenals van de gedocumenteerde instructies van de opdrachtgever. De uitkomsten van de controles moeten desgevraagd aan de opdrachtgever worden overlegd, voor zover deze relevant zijn voor de verwerking van de gegevens van de opdrachtgever. De controlemaatregelen worden beschreven in een gegevensbeschermingsconcept dat aan de opdrachtgever op verzoek moet worden overlegd.

3.9 De opdrachtnemer moet de opdrachtgever gelet op de aard van de verwerking en waar mogelijk met geschikte technische en organisatorische maatregelen helpen zijn verplichting om te voldoen aan verzoeken om behartiging van de in hoofdstuk III AVG genoemde rechten van de betrokken personen na te komen. De opdrachtgever moet de kosten dragen die hierbij voor de opdrachtnemer ontstaan.

3.10 De opdrachtnemer moet de opdrachtgever gelet op de aard van de verwerking en de informatie waarover hij beschikt, ondersteunen bij het naleven van de in art. 32 tot 36 AVG genoemde plichten.

4 Technische en organisatorische maatregelen ten behoeve van gegevensveiligheid

4.1 De opdrachtnemer neemt adequate technische en organisatorische maatregelen ter bescherming van de gegevens (vgl. art. 32 AVG). De opdrachtnemer is in het bijzonder verplicht de in Bijlage 2 bij deze overeenkomst contractueel overeengekomen technische en organisatorische maatregelen uit te voeren. Deze maatregelen moeten door de opdrachtnemer in de loop van de opdracht worden aangepast aan de technische en organisatorische ontwikkeling, zonder daarbij het beschermingsniveau te verlagen. Essentiële wijzigingen moeten schriftelijk worden overeengekomen.

4.2 De opdrachtgever levert de opdrachtnemer op verzoek het bewijs dat deze de technische en organisatorische maatregelen daadwerkelijk heeft genomen.

4.3 De opdrachtnemer is verplicht een adequate documentatie van de gegevensverwerking bij te houden, aan de hand waarvan aan de opdrachtgever de correcte gegevensverwerking kan worden bewezen. Het bewijs kan ook worden geleverd door middel van een goedgekeurde certificeringsprocedure conform art. 42 AVG.

5 Onderaannemer

5.1 De opdrachtnemer wordt hiermee toegestaan de in Bijlage 1 genoemde onderaannemers in te schakelen.

5.2 Het inschakelen van andere onderaannemers wordt hiermee algemeen toegestaan. De opdrachtnemer zal de opdrachtgever echter informeren over elke beoogde wijziging met betrekking tot het inschakelen of vervangen van onderaannemers; de opdrachtgever kan tegen de beoogde wijzigingen protest aantekenen. Diensten die de opdrachtnemer door derden als nevendienst ter ondersteuning bij de uitvoering van de opdracht laat verrichten, worden niet beschouwd als onderaanneming in de zin van deze regeling. Hiertoe behoren bijv. telecommunicatiediensten, schoonmakers, auditors of de afvoer van gegevensdragers. De opdrachtnemer is echter verplicht om ook bij extern uitbestede nevendiensten passende en wettelijke contractuele overeenkomsten aan te gaan en controlemaatregelen te nemen om de bescherming en veiligheid van de gegevens van de opdrachtgever te waarborgen.

5.3 Als de opdrachtnemer gebruikmaakt van een onderaannemer, moet de opdrachtnemer ervoor zorgen dat deze door middel van (i) een tussen de onderaannemer en de opdrachtnemer te sluiten overeenkomst of (ii) een ander juridisch instrument in de zin van de Europese wetgeving inzake gegevensbescherming aan dezelfde verplichtingen inzake gegevensbescherming moet voldoen als de opdrachtnemer in het kader van deze overeenkomst worden opgelegd. Hierbij moet de opdrachtnemer er in het bijzonder voor zorgen dat de onderaannemer voldoende garanties biedt dat de passende technische en organisatorische maatregelen zodanig worden uitgevoerd dat de verwerking van persoonsgegevens plaatsvindt in overeenstemming met de vereisten van de AVG. Op schriftelijk verzoek van de opdrachtgever zal de opdrachtnemer de opdrachtgever informatie verstrekken over de essentiële inhoud van de overeenkomst en de implementatie van de verplichtingen inzake gegevensbescherming in de onderaannemingsovereenkomst, zo nodig door inzage in de relevante contractuele documenten te verschaffen. Commerciële voorwaarden mag de opdrachtnemer daarbij weglakken. De opdrachtgever is verplicht tot geheimhouding van de verkregen informatie.

6 Controlerechten

6.1 De opdrachtgever heeft het recht om de nakoming van de verplichtingen die voortvloeien uit deze overeenkomst (inclusief de verstrekte instructies) zelf te controleren of te laten controleren door een geschikte derde die door de opdrachtgever is aangewezen.

6.2 De opdrachtnemer garandeert de opdrachtgever adequate ondersteuning bij de controles. In het bijzonder garandeert de opdrachtnemer toegang tot de gegevensverwerkende installaties en verstrekt hij de noodzakelijke informatie.

6.3 Ingeval een controle tot de conclusie leidt dat de opdrachtnemer en/of de verwerking niet voldoen aan de voorschriften van deze overeenkomst en/of de Europese wetgeving inzake gegevensbescherming, zal de opdrachtnemer alle corrigerende maatregelen nemen die nodig zijn om te garanderen dat aan de voorschriften van deze overeenkomst en/of de Europese wetgeving inzake gegevensbescherming wordt voldaan.

6.4 De kosten die door het uitvoeren van een controle voor de opdrachtgever ontstaan, dient deze zelf te dragen. De kosten die voor de opdrachtnemer ontstaan door het uitvoeren van een controle door de opdrachtgever, kan hij terugvorderen van de opdrachtgever indien de opdrachtgever meer dan één keer per kalenderjaar een controle uitvoert resp. laat uitvoeren.

6.5 Controles bij de opdrachtnemer moeten tijdig worden aangekondigd en mogen de bedrijfsactiviteiten van de opdrachtnemer niet disproportioneel belemmeren.

7 Kennisgevingsverplichtingen

De opdrachtnemer informeert de opdrachtgever onmiddellijk als een instructie van de opdrachtgever naar de mening van de opdrachtnemer in strijd is met de Europese wetgeving inzake gegevensbescherming. De terecht betwiste instructie hoeft niet te worden opgevolgd zolang deze niet door de opdrachtgever wordt gewijzigd of uitdrukkelijk wordt bevestigd. De opdrachtnemer is niet verplicht instructies materieelrechtelijk te controleren.

De opdrachtnemer dient de opdrachtgever onmiddellijk op gepaste wijze te informeren als er fouten of onregelmatigheden in de gegevensverwerking worden geconstateerd of als er een vermoeden van een inbreuk op de gegevensbescherming bestaat (hierna samen een "**incident**"). De opdrachtgever moet het incident documenteren, inclusief alle omstandigheden van de zaak, de gevolgen ervan en alle herstelmaatregelen, en op verzoek van de opdrachtgever deze gedocumenteerde informatie onmiddellijk schriftelijk of elektronisch aan de opdrachtgever zenden.

8 Aansprakelijkheid en vrijstelling

8.1 De opdrachtnemer is aansprakelijk voor schade die is veroorzaakt door opzet en/of grove nalatigheid van de opdrachtnemer of door hem ingeschakelde derden. Voor schade die het gevolg is eenvoudige nalatigheid van de opdrachtnemer of door hem ingeschakelde derden, is de opdrachtnemer alleen aansprakelijk voor zover er een kardinale verplichting wordt geschonden. Kardinale verplichtingen zijn essentiële contractuele verplichtingen die een correcte uitvoering van de overeenkomst pas mogelijk maken en op de nakoming waarvan de opdrachtgever heeft vertrouwd en mocht vertrouwen. In geval van eenvoudige nalatigheid met betrekking tot de schending van dergelijke kardinale verplichtingen blijft de aansprakelijkheid van de opdrachtnemer beperkt tot de normaliter voorzienbare schade.

8.2 De opdrachtgever vrijwaart de opdrachtnemer van alle aanspraken van derden (inclusief betrokkenen en/of gegevensbeschermingsautoriteiten), schade en kosten die berusten op een overtreding van de bepalingen van deze overeenkomst en/of van de Europese wetgeving inzake gegevensbescherming door de opdrachtgever; dit geldt niet als de opdrachtgever niet verantwoordelijk was voor deze overtreding of als de opdrachtnemer aan de overtreding heeft bijgedragen.

9 Looptijd

De looptijd van deze overeenkomst komt overeen met de looptijd van de hoofdovereenkomst. Bij beëindiging van de hoofdovereenkomst, om welke reden dan ook, wordt deze overeenkomst automatisch beëindigd. Opzegging om belangrijke redenen blijft onverlet.

10 Overig

10.1 De diensten van de opdrachtnemer in het kader van deze overeenkomst worden betaald via het vergoedingssysteem dat in de hoofdovereenkomst is geregeld.

10.2 Als persoonsgegevens van de opdrachtgever bij de opdrachtnemer in gevaar worden gebracht door maatregelen van derden (bijvoorbeeld door beslaglegging of inbeslagname), door een faillissement of crediteurenakkoord dan wel door andere vergelijkbare gebeurtenissen, moet de opdrachtnemer de opdrachtgever onmiddellijk informeren.

10.3 Indien afzonderlijke bepalingen van deze overeenkomst nietig zijn of worden, heeft dit geen invloed op de geldigheid van de overige bepalingen. In geval van nietigheid van een clausule zullen de partijen overeenstemming bereiken over een vervangende bepaling die inhoudelijk en economisch gezien aansluit bij het doel van de overeenkomst.

10.4 In het geval Groot-Brittannië uittreedt uit de Europese Unie verbindt de opdrachtnemer zich ertoe om reeds thans alle overeenkomsten te sluiten en alle handelingen te verrichten die nodig zijn om de contractuele gegevensverwerking in Groot-Brittannië vanaf het tijdstip van uittreding vorm te geven in overeenstemming met de geldende wetgeving inzake gegevensbescherming. Indien er op het tijdstip van uittreding geen positieve beslissing van de Europese Commissie over het passende beschermingsniveau bestaat, zijn dit vanuit het huidige perspectief met name standaardbepalingen inzake gegevensbescherming op grond van artikel 46, lid 2 c) voor de overdracht van persoonsgegevens aan verwerkers die gevestigd zijn in derde landen waar een passend beschermingsniveau niet gewaarborgd is.

Indien de opdrachtnemer deze verplichtingen niet nakomt, heeft de opdrachtgever het recht van de opdrachtnemer met ingang van het tijdstip van uittreding van Groot-Brittannië uit de Europese Unie te eisen dat de betreffende diensten worden verleend door een gelieerde onderneming of een onderneming met permanente hoofdvestiging op het grondgebied van de Europese Unie, zonder dat hierdoor voor de opdrachtgever extra inspanningen of kosten ontstaan.

10.5 Deze opdrachtverwerkingsovereenkomst is beschikbaar in 18 taalversies, waarbij de Duitse originele versie voorrang heeft in geval van afwijkingen.

10.6 Deze overeenkomst is onderworpen aan het recht van de Bondsrepubliek Duitsland, met uitsluiting van het VN-kooprecht. Exclusief bevoegde rechtbank is München.

10.7 De volgende bijlagen maken deel uit van deze overeenkomst:

Bijlage 1 – Beschrijving van de opdrachtverwerking
Bijlage 2 – Technische en organisatorische maatregelen

BIJLAGE 1 – Beschrijving van de opdrachtverwerking

1 Hoofdovereenkomst

De hoofdovereenkomst in de zin van punt 2.1 van het hoofddeel van de overeenkomst zijn de "Algemene voorwaarden voor gebruik van het platform".

Titel / partijen: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 München, Duitsland / **gebruiker**

2 Onderwerp en duur van de opdracht

Het onderwerp van de opdracht blijkt uit punt 1 (*Onderwerp*) en punt 8 (*Gegevens van de gebruiker en gegevensbescherming*) van de hoofdovereenkomst; de duur van de opdracht blijkt uit punt 7 (*Afsluiting van de overeenkomst, duur van de overeenkomst en opzeggingsrechten*) van de hoofdovereenkomst.

3 Omvang, aard en doel van de gegevensverwerking / maatregelen voor gegevensverwerking

Omvang, aard en doel van de verwerking van persoonsgegevens blijken uit punt 8 van de hoofdovereenkomst.

Nadere beschrijving van het onderwerp van de overeenkomst in termen van omvang, aard en doel:

Om de door de opdrachtnemer aangeboden diensten (zoals gedefinieerd in de hoofdovereenkomst) te kunnen aanbieden, moet de opdrachtnemer via verbonden voertuigen of mobiele apparaten persoonsgegevens van de opdrachtgever (en evt. overgedragen persoonsgegevens van een derde aanbieder waarmee de gebruiker derde diensten is overeengekomen) in de voor de levering van de diensten vereiste hoeveelheid verzamelen en deze overbrengen naar het platform van de opdrachtnemer en aldaar opslaan. De opdrachtnemer zal de gegevens die op het platform zijn opgeslagen, verwerken in de omvang die voor het leveren van de dienst noodzakelijk is (bijvoorbeeld om aan de hand van persoonsgegevens het rijgedrag van chauffeurs en het gebruik van het verbonden voertuig of mobiele apparaat te analyseren en te evalueren en de opdrachtgever op basis daarvan speciaal op hem afgestemde aanbiedingen te doen zoals chauffeurstrainingen, uitrustingsdetails en voorstellen om de efficiëntie te verhogen). Precieze omvang, aard en doel blijken in het bijzonder uit de aanvullend af te sluiten afzonderlijke overeenkomsten.

4 Groep van betrokkenen (categorieën van betrokken personen)

De opdrachtverwerking heeft betrekking op de volgende groepen personen:

- **chauffeurs en overige medewerkers** (medewerkers van de eigen vennootschap van de opdrachtgever), bijv. werknemers, leerlingen, sollicitanten, voormalige werknemers*;*
- **chauffeurs** die geen medewerker zijn;

- **contactpersonen** van verladers/lossers of andere zakenpartners van de opdrachtgever; en
- **concernmedewerkers** (medewerkers van een andere vennootschap uit de groep van de opdrachtgever).

5 Soort persoonsgegevens

De opdrachtverwerking omvat de volgende soorten persoonsgegevens:

- naam van de chauffeur en chauffeursidentificatienummer;
- voertuigidentificatienummer;
- standplaatsgegevens;
- gegevens over rij- en rusttijden;
- gegevens over het rijgedrag;
- toestandsgegevens van het verbonden voertuig;
- trailertoestandsgegevens;
- toestandsgegevens van op- en ingebouwde onderdelen, aggregaten en andere voertuigonderdelen;
- toestandsgegevens van evt. aangesloten IOT-apparaten;
- toestandsgegevens van mobiele apparaten;
- ladingsgegevens;
- opdrachtgegevens; en
- contactgegevens van contactpersonen van verladers/lossers of andere zakenpartners van de opdrachtgever.

6 Gedocumenteerde instructies

De opdrachtgever geeft de opdrachtnemer hiermee de opdracht om de persoonsgegevens als bedoeld in punt 8 van de hoofdovereenkomst te verwerken. Hierbij is in het bijzonder de volgende verwerking inbegrepen:

- De persoonsgegevens worden via het verbonden voertuig of mobiele apparaat overgebracht naar het cloudgebaseerde platform van de opdrachtnemer en daar opgeslagen.
- De persoonsgegevens worden uit hoofde van deze overeenkomst alleen verwerkt voor zover dit noodzakelijk is voor de nakoming van de hoofdovereenkomst; punt 8.3.4 van de hoofdovereenkomst blijft onverlet.
- De opdrachtnemer geeft de persoonsgegevens door aan een derde aanbieder (zoals gedefinieerd in de hoofdovereenkomst) indien en voor zover een dergelijke doorgifte aan de derde aanbieder nodig is om ervoor te zorgen dat deze zijn derde diensten (zoals gedefinieerd in de hoofdovereenkomst) aan de opdrachtgever kan leveren.
- De opdrachtnemer zal aan de hand van de persoonsgegevens het rijgedrag van de chauffeurs en het gebruik van het verbonden voertuig of mobiele apparaat analyseren en evalueren en de opdrachtgever

op basis daarvan speciaal op hem afgestemde aanbiedingen doen zoals chauffeurstrainingen, uitrustingsdetails en voorstellen om de efficiëntie te verhogen.

7 Plaats van verwerking

- Duitsland.
- Verenigd Koninkrijk; voor zover er gegevens worden verwerkt ten behoeve van IT-hosting en/of IT-support binnen de Europese Unie, zijn er opdrachtverwerkingsovereenkomsten gesloten.
- Indien de opdrachtnemer ten behoeve van IT-hosting en/of IT-support onderaannemers buiten de Europese Unie inzet (zie daarvoor punt 8 van deze Bijlage 1), vindt de doorgifte van persoonsgegevens plaats op basis van de tussen de opdrachtnemer en de onderaannemer afgesloten standaardcontractbepalingen/standaardbepalingen inzake gegevensbescherming voor de overdracht van persoonsgegevens aan verwerkers die gevestigd zijn in derde landen conform art. 46 lid 2 c) AVG.

8 Onderaannemer

De opdrachtnemer zet de volgende onderaannemers in (die evt. andere onderaannemers kunnen inzetten):

Nr.	Onderaannemer (firma, adres, contactpersoon)	Verwerkte gegevenscategorieën	Verwerkingsstappen / doel van de opdrachtverwerking in onderaanneming
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, Verenigde Staten	Alle persoonsgegevens van het platform die te maken hebben met het verkoopgedeelte (d.w.z. waar een klant zich op het platform kan registreren en bestellingen kan plaatsen)	Platform-hosting
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, Verenigde Staten	Alle persoonsgegevens van het platform die te maken hebben met het verkoopgedeelte (d.w.z. waar een klant zich op het platform kan registreren en bestellingen kan plaatsen)	IT-support voor platform
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 USA https://aws.amazon.com/de/compliance/contact/	Alle overige persoonsgerelateerde gebruikersgegevens die via het voertuig worden doorgegeven aan de opdrachtnemer	Platform-hosting / IT-support voor platform-hosting
4	Evt. in de toekomst in plaats van nr. 3: Amazon Webservices (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226, Verenigde Staten USA https://aws.amazon.com/de/compliance/contact/	Alle overige persoonsgerelateerde gebruikersgegevens die via het voertuig worden doorgegeven aan de opdrachtnemer	Platform-hosting

5	MAN Service und Support GmbH Dachauer Straße 667 D - 80995 München, Duitsland Duitsland	Alle persoonsgegevens die nodig zijn voor de bewerking van aanvragen van klanten in het kader van de 1st en 2nd level-support	1st level support
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403, Verenigde Staten USA	Alle persoonsgegevens die nodig zijn voor de bewerking van facturering/opdrachtafhandeling	Platform-hosting (EU Tenant – Gehost door Amazon Web Services (EU) – zie punt 4
7	MAN Truck & Bus AG Dachauer Str. 667 D - 80995 München, Duitsland Duitsland	Alle overige persoonsgerelateerde gebruikersgegevens die via het verbonden voertuig en/of mobiele apparaat worden doorgegeven aan de opdrachtnemer	Platform-hosting
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main, Duitsland Duitsland	Alle overige persoonsgerelateerde gebruikersgegevens die via TBM1/2-voertuigen worden doorgegeven aan de opdrachtnemer	Platform-hosting
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Zweden	Alle overige persoonsgerelateerde gebruikersgegevens die via het voertuig worden doorgegeven aan de opdrachtnemer	Platform-hosting
10	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hannover | Duitsland Duitsland	Alle overige persoonsgerelateerde gebruikersgegevens die via het voertuig worden doorgegeven aan de opdrachtnemer	Platform-hosting

BIJLAGE 2 – Technische en organisatorische maatregelen
De technische en organisatorische maatregelen die door de opdrachtnemer moeten worden genomen om een adequaat beschermingsniveau voor het risico te garanderen, worden beschreven in het gegevensbeschermingsconcept voor het RIO-platform en omvatten in het bijzonder:

1. Pseudonimisering

Voor zover de persoonsgegevens worden gebruikt voor evaluatiedoeleinden die ook kunnen worden bereikt met gepseudonimiseerde gegevens, worden pseudonimiseringstechnieken gebruikt. Hierbij wordt eerst voor elk gegevensveld vooraf gedefinieerd of het moet worden gepseudonimiseerd omdat er conclusies met betrekking tot een persoon uit kunnen worden getrokken. De pseudonimiseringssleutels worden opgeslagen in een “data safe”, waarvoor een zo hoog mogelijke toegangsbeperking wordt ingesteld.

2. Versleuteling

De mobiele eindapparaten communiceren versleuteld met het eindpunt door middel van een apparaatspecifiek apparaatcertificaat. De gegevens worden binnen het RIO-platform versleuteld doorgetransporteerd (“ubiquitous encryption” of “encryption everywhere”).

3. Waarborging van de vertrouwelijkheid

Alle medewerkers zijn en worden gewezen op hun zwijgplicht en schriftelijk verplicht tot geheimhouding van gegevens.

De gebruikte IT-infrastructuur wordt door Amazon Web Services (hierna AWS) in het kader van een cloud (IaaS & PaaS) beschikbaar gesteld. De toegangscontrole wordt beschikbaar gesteld door de exploitant van de AWS-datacenters: de uiterst veilige AWS-datacenters maken gebruik van elektronische bewakingsmaatregelen volgens de huidige stand van de techniek en multi-level toegangscontrolesystemen. De datacenters zijn 24 uur per dag bemand met getraind beveiligingspersoneel en de toegang ervan wordt strikt verleend volgens het principe van de minste rechten en uitsluitend ten behoeve van het systeembeheer.

De toegang tot de hardwarecomponenten (clients) bij TB Digital Services GmbH vindt plaats in overeenstemming met geldende standaardmaatregelen die voor elk specifiek geval geschikt zijn. Dit zijn bijv. toegangsbeperkingen door middel van toegangspoortjes (tourniquets), videobewakingssystemen, alarminstallatie en/of beveiligingsdienst, elektronisch of mechanisch beveiligde deuren, inbraakwerende gebouwen, gedocumenteerde toegangsrechten (bezoekers, extern personeel) of aangegeven veiligheidszones.

De toegangscontroles omvatten maatregelen voor apparaatbeveiliging, netwerkbeveiliging en applicatiebeveiliging.

Als maatregelen voor de apparaatbeveiliging in het voertuig worden verschillende maatregelen geïmplementeerd: de mobiele eindapparaten zijn vast in het voertuig ingebouwd en beschikken over secure

boot, d.w.z. er bestaat geen mogelijkheid om een extern besturingssysteem te laden en te starten. De mobiele eindapparaten communiceren versleuteld met het eindpunt door middel van een apparaatspecifiek apparaatcertificaat. De gegevens worden binnen het RIO-platform versleuteld doorgetransporteerd ("ubiquitous encryption" of "encryption everywhere"). De eindapparaten zijn door het regelmatig toepassen van veiligheidsupdates op de huidige stand van beveiliging (patchmanagement).

Als maatregelen voor de netwerkbeveiliging worden eveneens verschillende standaardmaatregelen geïmplementeerd: Er worden adequate wachtwoordspecificaties (volgens de stand van de techniek) geïmplementeerd (wachtwoordlengte, -complexiteit, -geldigheidsduur, etc.). Herhaalde foutieve invoer van de combinatie van gebruikersnaam en wachtwoord leidt tot een (tijdelijke) blokkering van de gebruikersnaam. Het bedrijfsnetwerk is door middel van een firewall afgeschermd van onveilige open netwerken. Er is een proces ingesteld dat ervoor zorgt dat de mobiele apparaten regelmatig worden voorzien van beveiligingsupdates (OTA-proces). Voor het detecteren of voorkomen van aanvallen op het bedrijfsnetwerk (intranet) worden geschikte technologieën gebruikt (bijv. intrusion detection systemen). De medewerkers worden regelmatig bewust gemaakt van de gevaren en risico's.

Als maatregelen voor de applicatiebeveiliging worden enkele standaardmaatregelen geïmplementeerd:

De relevante applicaties zijn door middel van geschikte authenticatie- en autorisatiemechanismen beveiligd tegen onbevoegde toegang. Er worden adequate wachtwoordspecificaties (volgens de stand van de techniek) geïmplementeerd (wachtwoordlengte, -complexiteit, -geldigheidsduur, etc.). Voor applicaties die speciale bescherming behoeven, worden sterke authenticatiemechanismen gebruikt (bijv. tokens, PKI). Herhaalde foutieve invoer van de combinatie van gebruikersnaam en wachtwoord leidt tot een (tijdelijke) blokkering van de gebruikersnaam. De in het relevante proces gebruikte gegevens worden in versleutelde vorm opgeslagen op een mobiel gebruikte gegevensdrager. De toegangen en toegangspogingen tot de applicaties die hebben plaatsgevonden, worden vastgelegd. De aangemaakte logbestanden worden gedurende een geschikte periode (minimaal 90 dagen) bewaard en (steekproefsgewijs) gecontroleerd.

Gebruikersrechten (voor toegang tot installaties en programma's) worden beveiligd met verschillende maatregelen, waarbij deze in principe worden toegewezen aan een definieerbare persoon. Het toekennen van de rechten is de verantwoordelijkheid van de platformbeheerder en wordt regelmatig gecontroleerd. De toewijzing van de toegangsrechten vindt uitsluitend plaats volgens een gedefinieerd en gedocumenteerd proces. Wijzigingen in de toegangsrechten worden aangebracht volgens het vierogenprincipe en worden gedocumenteerd in een van een versienummer voorzien logbestand.

Als maatregelen voor de toegangscontrole resp. -besturing worden verschillende maatregelen geïmplementeerd: de toegangsrechten worden gedefinieerd en gedocumenteerd in het kader van een rol-/autorisatieconcept en worden overeenkomstig de taakspecifieke vereisten toegewezen aan de betreffende rollen. Er zijn specifieke rollen/rechten ingesteld voor technische beheerders (die, voor zover technisch mogelijk, geen toegang verlenen tot persoonlijke informatie). Er zijn specifieke rollen/rechten ingesteld voor de technische ondersteuning (die geen technische beheerdersrechten inhouden).

De definitie van rollen/rechten en de toewijzing van rollen/rechten vindt, voor zover technisch en organisatorisch mogelijk, plaats door verschillende personen en volgens een controleerbare (goedkeurings)procedure en voor een beperkte tijd. Directe toegang tot de database buiten het rol-/autorisatieconcept om is alleen mogelijk voor geautoriseerde databasebeheerders. Er is een regeling voor het gebruik van private gegevensdragers of het gebruik van private gegevensdragers is verboden. Er zijn bindende voorschriften met betrekking tot gegevenstoegang voor extern onderhoud, onderhoud op afstand en telewerken. Vernietiging/verwijdering van documenten en gegevensdragers (bijv. shredder, gegevensbeschermingsbak) vindt plaats volgens de eisen van de gegevensbescherming en door betrouwbare verwijderingsbedrijven.

Het rol-/autorisatieconcept wordt regelmatig aangepast aan de veranderende structuren van de werkorganisatie (bijv. nieuwe rollen) en de toegewezen rollen/rechten worden regelmatig gecontroleerd (bijv. door de chefs) en indien nodig aangepast of ingetrokken. Er vindt regelmatig centrale controle plaats met betrekking tot toegewezen standaardprofielen. Het gebruik van de toegang voor wijzigingen (opslaan, wissen) wordt geregistreerd en de aangemaakte logbestanden worden gedurende een geschikte periode (minimaal 90 dagen) bewaard en (steekproefsgewijs) gecontroleerd.

Als algemene maatregelen voor de beveiliging van de overdracht worden verschillende standaardmaatregelen geïmplementeerd:

De personen die zijn belast met de overdracht, worden van tevoren vertrouwd gemaakt met de te nemen beveiligingsmaatregelen. De groep van ontvangers is vooraf gedefinieerd, zodat een hierbij passende controle (authenticatie) mogelijk is. Het gehele proces van de gegevensoverdracht is vastgelegd en gedocumenteerd en de uitvoering van de concrete gegevensoverdracht wordt geregistreerd of gedocumenteerd (bijv. ontvangstbevestiging, beantwoording). De personen die zijn belast met de overdracht, voeren van tevoren een controle op geldigheid, volledigheid en correctheid uit.

Voorafgaand aan de uitvoering van de concrete gegevensoverdracht vindt een controle van het ontvangersadres plaats (bijv. e-mailadres). De overdracht van gegevens via het internet vindt plaats in versleutelde vorm (bijv. bestandsversleuteling). De integriteit van de overgedragen gegevens wordt, voor zover technisch mogelijk, gewaarborgd door het gebruik van ondertekeningsprocedures (digitale handtekening). Elektronische ontvangstbevestigingen worden in een gepaste vorm gearchiveerd. Ongewenste gegevensoverdracht via internet wordt voorkomen door middel van geschikte technologieën (bijv. proxy, firewall).

Verder worden als maatregelen voor de uitvoering van de scheidingsvereiste de volgende standaardmaatregelen geïmplementeerd:

Er zijn bindende voorschriften met betrekking tot het doel van de verwerking om te voldoen aan de scheidingsvereiste. De gegevens die voor bepaalde doeleinden zijn verzameld, worden gescheiden opgeslagen van gegevens die voor andere doeleinden zijn verzameld. De gebruikte IT-systemen staan gescheiden opslag van gegevens toe (via multi-client-functionaliteit of toegangsconcepten). Er vindt scheiding van gegevens plaats

in test- en productieve systemen. Voor gepseudonimiseerde gegevens wordt de sleutelcode die opnieuw identificeren mogelijk maakt, gescheiden opgeslagen of bewaard. Bij de opdrachtverwerking of functieoverdracht worden de gegevens van verschillende opdrachtgevers bij de opdrachtnemer gescheiden verwerkt. De bestaande rol-/autorisatieconcepten maken door hun vormgeving de logische scheiding van de verwerkte gegevens mogelijk.

4. Waarborging van de integriteit

Als maatregelen voor de uitvoering van de invoerregistratie worden verschillende standaardmaatregelen geïmplementeerd:

Wijzigingen van de toegangsrechten en alle beheerdersactiviteiten worden geregistreerd. Het gebruik van de toegang voor schrijven (invoeren, wijzigen, wissen) en wijzigen in de gegevensvelden wordt geregistreerd (bijv. de inhoud van een nieuw ingevoerd of gewijzigd gegevensrecord). Er vindt logboekregistratie plaats van overdrachten (bijv. downloads) en van logins.

Ten behoeve van de traceerbaarheid van de invoer worden de gebruikte registratiegegevens gedocumenteerd en gearchiveerd. De logboekregistratie vindt plaats met datum en tijd, gebruiker, soort activiteit, applicatieprogramma en volgnummer van het gegevensrecord. De instellingen voor logboekregistratie worden gedocumenteerd.

Tot de logbestanden wordt uitsluitend een alleen-lezen-toegang verleend. De groep met toegangsrechten tot de logbestanden is zeer beperkt (bijv. tot de beheerder, de functionaris voor gegevensbescherming, de revisor). De logbestanden worden gedurende een vastgelegde periode (bijv. 1 jaar) bewaard en vervolgens volgens de eisen van de gegevensbescherming gewist. De logbestanden worden regelmatig automatisch geëvalueerd. Evaluaties van de logbestanden worden voor zover mogelijk in gepseudonimiseerde vorm gemaakt.

5. Waarborging van de beschikbaarheid

De architectuur is door interne replicatiemechanismen binnen het AWS-platform als zodanig beveiligd tegen gegevensverlies. Verder worden er als maatregelen voor de objectbeveiliging de volgende standaardmaatregelen van AWS geïmplementeerd:

Er worden brandbeveiligingsmaatregelen genomen (bijv. brandwerende deuren, rookmelders, brandschotten, rookverbod). De computersystemen zijn beschermd tegen overstromingen (bijv. computerruimte op de eerste verdieping, watermelders). Er worden maatregelen genomen om schokken te voorkomen (bijv. computerruimte niet nabij hoofdwegen, treinrails, machinekamers). De computersystemen zijn beveiligd tegen elektromagnetische velden (bijv. stalen platen in de buitenmuren). Er worden maatregelen genomen tegen vandalisme en diefstal (vgl. toegangscontrole). De computersystemen bevinden zich in geklimatiseerde ruimten (temperatuur en luchtvochtigheid worden geregeld door het airconditioningssysteem). De computersystemen moeten met een overspanningsbescherming worden beveiligd tegen overspanningspieken. Er worden

maatregelen genomen om te zorgen voor een storingsarme en constante stroomvoorziening (bijv. UPS-apparaten, noodstroomaggregaten).

De gegevensbestanden worden regelmatig veiliggesteld in de vorm van back-upkopieën binnen het AWS-platform. Het back-upconcept is gedocumenteerd en wordt regelmatig gecontroleerd en geactualiseerd. Back-upmedia zijn beveiligd tegen onbevoegde toegang. De gebruikte back-upprogramma's voldoen aan de huidige kwaliteitsstandaarden en worden wat dit betreft regelmatig geactualiseerd. Er is een redundantie-datacenter opgezet (ver van de plaats van verwerking) en in het geval van een ramp kan dit de verwerking van gegevens voortzetten. De verschillende maatregelen ten behoeve van de beschikbaarheidscontrole zijn gedocumenteerd in een calamiteitenbeheersplan van AWS.

Voordat er een opdracht voor gegevensverwerking wordt verleend, wordt de opdrachtnemer zorgvuldig en volgens vastgestelde criteria (technische en organisatorische maatregelen) gecontroleerd. Hiervoor wordt in het bijzonder een gedetailleerde beschrijving van de door de opdrachtnemer uitgevoerde technische/organisatorische maatregelen voor gegevensbescherming (beantwoording vragenlijst of gegevensbeschermingsconcept) gevraagd en gecontroleerd. Afhankelijk van de hoeveelheid en gevoeligheid van de verwerkte gegevens kan deze controle ook ter plaatse bij de opdrachtnemer worden uitgevoerd. Bij de selectie van opdrachtnemers wordt rekening gehouden met geschikte certificeringen (bijv. ISO 27001). De vaststelling van de geschiktheid van de opdrachtnemer wordt in een passende en begrijpelijke vorm gedocumenteerd.

Ter ondersteuning van de opdrachtrelatie wordt een opdrachtverwerkingsovereenkomst tussen de opdrachtgever en opdrachtnemer afgesloten. Hierin worden gedetailleerd en schriftelijk de competenties en verantwoordelijkheden alsmede de plichten van beide partijen vastgelegd. Als een gecontracteerde dienstverlener buiten de EU of de EER is gevestigd, worden de standaardcontractbepalingen van de EU toegepast. Er wordt contractueel vastgelegd dat de gegevensverwerking door de opdrachtnemer alleen mag plaatsvinden in het kader van instructies van de opdrachtgever. De opdrachtnemer is verplicht de opdrachtgever onmiddellijk te informeren als een van zijn instructies naar de mening van de opdrachtnemer in strijd is met de voorschriften van de gegevensbescherming. Om recht te doen aan de rechten van de betrokkenen, wordt in de opdrachtverwerkingsovereenkomst overeengekomen dat de opdrachtnemer de opdrachtgever naar behoren moet ondersteunen, voor zover dit bijv. in het geval van het verstrekken van informatie aan betrokkenen nodig is.

In het verdere verloop van de opdrachtverwerking controleert de opdrachtgever de werkresultaten van de opdrachtnemer op vorm en inhoud. De naleving van de bij de opdrachtnemer genomen technische en organisatorische maatregelen wordt regelmatig gecontroleerd. Hiervoor wordt voornamelijk gebruik gemaakt van het overleggen van actuele testcertificaten of geschikte certificeringen resp. van bewijzen van uitgevoerde IT-beveiligings- of gegevensbeschermingsaudits. Voor zover er onderaannemers worden ingezet, is contractueel bepaald dat deze op overeenkomstige wijze kunnen worden gecontroleerd.

6. Waarborging van de belastbaarheid van de systemen

De AWS-cloudinfrastructuur is opgezet als een van de meest flexibele en veiligste cloud computing omgevingen. Het ontwerp is gericht op optimale beschikbaarheid bij volledige scheiding van klanten. De infrastructuur biedt een uiterst schaalbaar, zeer betrouwbaar platform dat het klanten toestaat applicaties en inhoud indien nodig snel en veilig over de hele wereld te verspreiden. De AWS-services zijn in zoverre inhoudsonafhankelijk dat zij alle klanten hetzelfde hoge beveiligingsniveau bieden, ongeacht het type inhoud of de geografische regio waar de inhoud wordt opgeslagen.

De uiterst veilige AWS-datacenters van wereldklasse maken gebruik van elektronische bewakingsmaatregelen volgens de huidige stand van de techniek en multi-level toegangscontrolesystemen. De datacenters zijn 24 uur per dag bemand met getraind beveiligingspersoneel en de toegang ervan wordt strikt verleend volgens het principe van de minste rechten en uitsluitend ten behoeve van het systeembeheer.

7. Procedures voor het herstellen van de beschikbaarheid van persoonsgegevens na een fysiek of technisch incident

De AWS-datacenters worden in clusters in verschillende delen van de wereld gebouwd. Alle datacenters zijn online en bedienen klanten; geen enkel datacenter is uitgeschakeld. In het geval van een storing leiden geautomatiseerde processen het gegevensverkeer van klanten weg uit de getroffen gebieden. De kerntoepassingen worden geleverd in een N+1-configuratie, zodat er bij uitval van een datacenter voldoende capaciteit is om de lasten van het gegevensverkeer over de resterende locaties te verdelen.

AWS biedt de flexibiliteit om instanties te plaatsen en gegevens op te slaan in meerdere geografische regio's en ook in meerdere availability zones binnen de afzonderlijke regio’s. Elke availability zone is ontwikkeld als onafhankelijke uitvalzone. Dit betekent dat availability zones binnen een typische stadsregio fysiek zijn verdeeld en zich bijvoorbeeld bevinden in gebieden met een laag overstromingsrisico (afhankelijk van de regio zijn er verschillende categorieën overstromingszones). Naast een zelfstandige ononderbroken stroomvoorziening en noodstroomgeneratoren ter plaatse worden alle availability zones gevoed via verschillende stroomnetten van onafhankelijke stroomleveranciers om individuele storingspunten te minimaliseren. Alle availability zones zijn redundant verbonden met meerdere tier-1-transitproviders.

Het incidentmanagementteam van Amazon past standaard diagnostische procedures toe om bedrijfskritische incidenten op te lossen. Het bedrijfspersoneel biedt een constante bezetting, 24 uur per dag, 7 dagen per week en 365 dagen per jaar, om storingen op te sporen en de gevolgen en verhelping ervan te beheren.

8. Procedures voor het regelmatig controleren, beoordelen en evalueren van de effectiviteit van technische en organisatorische maatregelen

De in het bedrijf aanwezige richtlijnen en instructies resp. de geïmplementeerde normen voor informatiebeveiliging worden ook toegepast met betrekking tot de implementatie en de exploitatie van het RIO-

platform. Bedrijfsfuncties voor gegevensbescherming en informatiebeveiliging zijn aanwezig (functionaris voor gegevensbescherming en information security officer). Medewerkers worden verplicht tot geheimhouding van gegevens en worden via brochures, flyers, intranetinformatie, enz. geïnformeerd over gegevensbeveiligings- resp. IT-beveiligingsmaatregelen.

De interne processen worden op naleving van technische en organisatorische maatregelen voor gegevensbeveiliging gecontroleerd door middel van revisie, informatiebeveiliging en gegevensbescherming.

De verwerkingsprocessen en maatregelen voor gegevensbeveiliging worden gedocumenteerd in een lijst met verwerkingsactiviteiten. Er vindt regelmatig controle plaats (intern en extern) op de effectiviteit van de maatregelen.