Uppdragsdatabehandlingsavtal
(enligt artikel 28 GDPR)

mellan

användaren (enligt definitionen i huvudavtalet)

(hädanefter kallat ”**Uppdragsgivare**”)

och

TB Digital Services GmbH, Oskar Schlemmer-Strasse 19 - 21, D-80807 München

(hädanefter kallat ”**Uppdragstagare**”)
(Uppdragsgivaren och uppdragstagaren hädanefter var sin ”**Part**” och tillsammans ”**Parter**)

Preambel

(A) Detta uppdragsdatabehandlingsavtal (hädanefter ”**Avtal**”) är tillämpligt vid samtliga verksamheter där uppdragstagaren kommer i beröring med personuppgifter (som definierats i nummer 1.5 nedan) från uppdragsgivaren, från utomstående leverantörer eller andra berörda i samband med i nummer 2 beskriven verksamhet ur Allmänna ramvillkor för plattformsanvändning och, vid behov, därtill ingångna individuella avtal för ytterligare tjänster (hädanefter ”**Huvudavtal**”).

(B) Under detta avtal handlar uppdragsgivaren som personuppgiftsansvarig och uppdragstagaren som personuppgiftsbiträde inom ramen för en uppdragsbehandling enligt artikel 28 GDPR (enligt definitionen nedan).

Parterna överenskommer sålunda följande:

1 Definitioner och interpretation

1.1 ”**Europeisk lag**“ är den tillämpliga lagen i den europeiska unionen, tillämpliga lagar hos varje medlemsstat i den europeiska unionen liksom tillämpliga lagar hos varje enskild stat, som i efterhand kommer att bli medlemsstat i den europeiska unionen.

1.2 ”**Europeisk dataskyddslag**“ är den europeiska unionens lag för behandling av personuppgifter (särskilt GDPR), tillämpliga lager hos aktuella medlemsstater inom den europeiska unionen för behandling av personuppgifter (i synnerhet BDSG i dess respektive gällande version) liksom tillämpliga lagar hos varje enskild stat för behandling av personuppgifter, som i efterhand kommer att bli medlemsstat i den europeiska unionen.

1.3 ”**GDPR**“ är ”EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 från den 2016-04-27 till skydd av fysiska personer med avseende på behandling av personuppgifter, om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)“.

1.4 ”**BDSG**“ är Förbundsrepubliken Tysklands lag om dataskydd.

1.5 „**Personuppgifter**“ har betydelsen som definierats i BDSG/i DS-GVO.

2 Föremål för databehandlingen / Uppdragsgivarens åtaganden

2.1 Detta avtal reglerar parternas åtaganden i samband med behandlingen av personuppgifter från uppdragsgivaren genom uppdragstagaren inom ramen för i bilaga 1nämnda huvudavtal.

2.2 Behandlingens uppgift och längd, art och ändamål, personuppgifters art, berörda personers kategorier och den ansvariges åtaganden och rättigheter framgår ur bilaga 1 bilaga 1 i detta avtal och kravspecifikationen i huvudavtalet.

2.3 Uppdragsgivaren förblir personuppgiftsansvarig enligt GDPR och garanterar tillförlitligheten hos behandlingen av de berörda personernas personuppgifter (förare och eventuellt ytterligare personer). I detta avseende ska uppdragsgivaren i synnerhet fullgöra sin omfattande informationsskyldighet och säkerställa att det föreligger ett dataskyddsrättsligt stöd för behandlingen av de personrelaterade uppgifterna (t.ex. ingången driftsöverenskommelse, begränsning av behandlingen till anställningsförhållandet.

3 Uppdragstagarens åtaganden

3.1 Uppdragstagaren ska behandla uppdragsgivarens personuppgifter uteslutande för de i bilaga 1 nämnda ändamålen och inom ramen för huvudavtalet, liksom på uppdrag av och enligt i denna bilaga 1 dokumenterade direktiv från uppdragsgivaren; uppdragstagaren får inte behandla personuppgifterna enligt detta avtal för några andra ändamål. Av detta oberörd förblir behandlingen utanför detta avtal för egna ändamål enligt huvudavtalets nummer 8.3.4. Kopior och duplikat av personuppgifter får inte framställas utan uppdragsgivarens vetskap. Undantag från detta är säkerhetskopior, i den utsträckning de behövs för att garantera vederbörlig databehandling, liksom data, som är nödvändig med hänsyn till uppfyllande av lagstadgade arkiveringsplikter.

3.2 Efter avslutat tillhandahållande av behandlingstjänsterna ska uppdragstagaren enligt uppdragsgivarens val antingen återlämna uppdragsgivarens samtliga personuppgifter och/eller själv radera dem dataskyddsrättsligt korrekt, om inte lagstadgade arkiveringstider hindrar detta och uppdragstagaren inte behandlar dem för egna ändamål utanför detta avtal enligt nummer 8.3.4. i huvudavtalet. Detsamma gäller för test- och avfallsmaterial. Den fullständiga raderingen resp. utlämning av uppgifter till uppdragsgivaren ska på begäran skriftligt bekräftas till honom med datumuppgift.

3.3 I den mån detta ingår i leveransen ska uppdragstagaren understödja uppdragsgivaren vid fullgörandet av de berördas rättigheter (tillgång, rättelse, invändning, radering) enligt vederbörande instruktion från uppdragsgivaren.

3.4 Uppdragstagaren bekräftar, att han - om lagen kräver det - har utsett ett dataskyddsombud (jfr. § 38 BDSG, artikel 37 GDPR).

3.5 Uppdragstagaren åtar sig, att omedelbart meddela uppdragsgivaren resultatet från dataskyddstillsynsmyndigheten kontroll, såvida dessa står i samband med behandlingen av data från uppdragsgivaren. Eventuellt fastställda anmärkningar kommer uppdragstagaren inom skälig tid att åtgärda och meddela detta till uppdragsgivaren.

3.6 Behandlingen av data genom uppdragstagaren och de av uppdragsgivaren godkända underentreprenörer får uteslutande äga rum i Förbundsrepubliken Tysklands område, i en medlemsstat i den europeiska unionen eller i en annan fördragsslutande stats avtal via den europeiska ekonomiska regionen. Varje utlokalisering till ett annat land (hädanefter „**Tredjeland**“) kräver ett föregående uttryckligt godkännande från uppdragsgivaren och får dessutom enbart ske om de särskilda förutsättningarna för dataexport till tredjeland har uppfyllts (jfr. artikel 40 ff. GDPR). Härtill är uppgifter i bilaga 1 nödvändiga och kompletterande (avtals-) underlag vid behov bifogas.

3.7 Uppdragstagaren ska göra den personal som anlitas för genomförandet av arbetena förtrogen med de dataskyddsbestämmelser som gäller för dem samt ålägga dem tystnadsplikt (jfr. artikel 28.3b GDPR) samt med lämpliga åtgärder säkerställa att personalen bara behandlar personuppgifter på instruktion från uppdragstagaren.

3.8 Uppdragstagaren övervakar lagstiftade dataskyddade föreskrifters efterlevnad i detta avtal och de dokumenterade direktiven från uppdragsgivaren regelbunden under hela avtalstiden. Kontrollernas resultat ska på begäran redovisas för uppdragsgivaren, såvida dessa är relevanta för behandlingen av data från uppdragsgivaren. Åtgärderna för övervakning finns beskriven i ett dataskyddsansvarige, som på begäran ska redovisas för uppdragsgivaren.

3.9 Uppdragstagaren ska stödja uppdragsgivaren med tanke på artens behandling och, om möjligt, med lämpliga tekniska och organisatoriska åtgärder, efterkomma sin plikt gällande svar på framställningar om medvetenhet gällande i kapitel III DS-GVO omnämnda rättigheter hos berörda personer. Uppdragsgivaren ska i detta fall bära omkostnader som härvid uppstår för uppdragstagaren.

3.10 Uppdragstagaren ska stödja uppdragsgivaren med tanke på artens behandling och de honom till förfogande stående informationer vid efterlevnad av de i Art. 32 till 36 DS-GVO omnämnda plikter.

4 Tekniska och organisatoriska åtgärder för ADB-säkerhet

4.1 Uppdragstagaren ska vidta lämpliga tekniska och organisatoriska åtgärder för dataskyddet (jfr. artikel 32 GDPR). Uppdragstagaren är särskild förpliktad, att omsätta de i bilaga 2 till detta avtal avtalsenliga överenskomna tekniska och organisatoriska åtgärder. Dessa åtgärder ska av uppdragstagaren inom loppet av uppdrags förhållandet anpassas den tekniska och organisatoriska vidare utvecklingen, utan att därmed sänka skyddsnivån. Väsentliga ändringar ska överenskommas skriftligt.

4.2 Uppdragstagaren ska för uppdragsgivaren på förfrågan redovisa den faktiska efterlevnaden av tekniska och organisatoriska åtgärder.

4.3 Uppdragstagaren är förpliktad, att föra en rimlig dokumentation över databehandlingen, med vars hjälp uppdragsgivaren kan bevisa en korrekt tillämpning av databehandlingen. Bevisföring kan även ske genom ett godkänt certifieringsförfarande enligt Art. 42 DS-GVO.

5 Underentreprenörer

5.1 Härmed erhåller uppdragstagaren tillstånd att koppla in de i bilaga 1 omnämnda underentreprenörer.

5.2 Att koppla in ytterligare underentreprenörer är härmed generellt godkänd. Uppdragstagaren kommer emellertid att informera uppdragsgivaren över varje planerad ändring med avseende på att anlita eller ersätta underentreprenörer; uppdragsgivaren kan mot denna planerade ändring inlägga protest. Sådana tjänster, som uppdragstagaren anlitar hos tredje part som extratjänst till stöd för uppdragets genomförande, räknas inte som under uppdragsförhållande enligt denna reglerings mening. Till detta räknas bl.a. telekommunikationstjänster, städpersonal, kontrollanter eller avfallshantering av databärare. Uppdragstagaren är emellertid förpliktad, att garantera skydd och säkerhet för uppdragsgivarens uppgifter också vid tilldelade sidouppdrag, att träffa lämpliga och lagkonforma avtalsenliga överenskommelser, liksom kontrollåtgärder.

5.3 Om uppdragstagaren anlitar en underentreprenör, ska uppdragstagaren säkerställa, att denne i samband med (i) ett mellan underentreprenören och uppdragstagaren ingånget avtal eller (ii) ett ytterligare rättsligt instrument enligt EU:s dataskyddslagstiftning åläggs samma dataskyddsplikter som åläggs uppdragstagaren enligt detta avtal. Därvid ska uppdragstagaren särskilt säkerställa, att underentreprenören erbjuder tillräckliga garantier för att lämpliga tekniska och organisatoriska åtgärder kommer att vidtas för att behandlingen av personuppgifter sker i enlighet med kraven i GDPR. På skriftlig begäran från uppdragsgivaren kommer uppdragstagaren att ge uppdragsgivaren upplysning om det väsentliga avtalsinnehållet och omsättningen av dataskydssrelevanta åtaganden i underuppdragsförhållandet, vid behov genom insyn i relevanta avtalsunderlag. Kommersiella krav får uppdragstagaren här svärta. Uppdragsgivaren är förpliktad att hemlighålla erhållen information.

6 Kontrollrätt

6.1 Uppdragsgivaren har rätt att kontrollera respektive låta kontrollera, själv eller genom en av uppdragsgivaren utsett tredje person, att åtaganden ur detta avtal efterlevs (inklusive beviljade direktiv).

6.2 Uppdragstagaren lämnar uppdragsgivaren vid kontrollerna rimlig understöd. I synnerhet medger uppdragstagaren åtkomst till databehandlingsanläggningar och lämnar nödvändig information.

6.3 För den händelse att en kontroll kommer fram till ett resultat, att uppdragstagaren och/eller behandlingen inte motsvarar avtalets riktlinjer och/eller europeiska dataskyddsrätt, kommer uppdragstagaren att vidta samtliga korrekturåtgärder som krävs, för att efterleva och garantera avtalets riktlinjer och/eller europeiska dataskyddsrätten.

6.4 Kostnaderna, som uppstår för uppdragstagaren genom verkställande av kontrollen, ska han bära själv. Kostnaderna, som uppstår för uppdragstagaren genom verkställande av en kontroll genom uppdragsgivaren, kan han begära från uppdragsgivaren, om uppdragsgivaren begär en kontroll fler än en gång per kalenderår resp. låter göra.

6.5 Kontroller hos uppdragstagaren ska meddelas i tid och får inte oproportionerligt påverka uppdragstagarens affärsverksamhet.

7 Hänvisningsplikt

Uppdragstagaren informerar omgående uppdragsgivaren, när en av uppdragsgivarens direktiv enligt uppdragstagarens mening bryter mot europeisk dataskyddsrätt. Det med rätta påtalade direktiv behöver inte följas, så länge det inte ändras genom uppdragsgivaren eller uttryckligen bekräftas. Uppdragstagaren är inte förpliktad till en materiell-rättslig prövning av direktiven.

Uppdragstagaren ska vid fastställande av fel eller oregelbundenheter av databehandling eller vid misstanke av en dataskyddsöverträdelse (tillsammans hädanefter „**Händelse**“) omedelbart lämpligt informera uppdragsgivaren. Uppdragstagaren ska dokumentera händelsen inklusive alla faktiska omständigheter, dess påverkan och samtliga åtgärder för avhjälpande och på uppdragsgivarens begäran omedelbart skriftligt eller elektroniskt överlämna denna dokumenterade information till uppdragsgivaren.

8 Ansvar och avsked

8.1 Uppdragstagaren ansvarar för skador, som genom uppsåt och/eller grov vårdslöshet åstadkommits av uppdragstagaren eller hans agenter. För skador, som beror på enkel vårdslöshet av uppdragstagaren eller hans agenter, ansvarar uppdragstagaren bara, såvitt en kardinalplikt kränkts. Kardinalplikter är väsentliga avtalsplikter, som en korrekt genomförbarhet av avtalet först möjliggör och på vars fullgörande uppdragsgivaren har litat och kunde lita på. Vid enkel vårdslöshet beträffande kränkning av sådan kardinalplikt, är uppdragstagarens ansvar begränsat till typiskt förutsebara skador.

8.2 Uppddragsgivaren friställer uppdragstagaren från samtliga anspråk från tredje person (inklusive berörda personer och/eller dataskyddsmyndigheter), skador och omkostnader, som beror på en överträdelse från uppdragsgivaren mot bestämmelser i detta avtal och/eller mot europeiskt dataskyddsrätt, detta gäller inte, om uppdragsgivaren inte har gjort sig skyldig till överträdelsen eller såvida uppdragstagaren har bidragit till överträdelsen.

9 Löptid

Avtalets löptid motsvarar huvudavtalets löptid. Vid huvudavtalets avslutande, av vilken anledning det må vara, kommer detta avtal automatiskt att avslutas. Uppsägningen av viktig anledning förblir oberörd.

10 Övrigt

10.1 Uppdragstagarens tjänster, enligt detta avtal, har kompenserats genom andra ersättningar i huvudavtalet.

10.2 Om uppdragsgivarens personuppgifter hos uppdragstagaren äventyras genom åtgärder från tredje person (till exempel utmätning eller beslag), genom insolvens eller ackordsförfarande eller genom andra jämförbara händelser hotad, ska uppdragstagaren omedelbart informera uppdragsgivaren.

10.3 Skulle enskilda bestämmelser i detta avtal vara eller bli verkningslös, berör det inte effekten av övriga bestämmelser. Parterna kommer, i händelse av en klausuls verkningslöshet, att enas om en i saklig och ekonomiskt hänseende, på avtalets ändamål orienterade ersättningsreglering.

10.4 För den händelse, att Storbritannien lämnar den europeiska unionen, förpliktar sig uppdragstagaren redan nu att avsluta samtliga överenskommelser och verkställande av alla handlingar som är nödvändig, för att acceptabelt utforma avtalets databehandling i Storbritannien från och med utträdets tidpunkt. Om det vid utträdestidpunkten inte finns något positivt beslut om adekvat skyddsnivå från EU-kommissionen är detta i dagens läge i synnerhet standardiserade dataskyddsbestämmelser enligt artikel 46.2c för överföring av personuppgifter till personuppgiftsbiträden som är etablerade i tredjeländer, där ingen skälig skyddsnivå garanteras.

Uppfyller uppdragstagaren inte dessa åtaganden, äger uppdragsgivaren rätt, att kräva från uppdragstagaren med verkan från Storbritanniens utträde ur den europeiska unionen, att berörda tjänster ska tillhandahållas av ett allierat företag resp. av en företagsdel med ständigt säte i den europeiska unionens område, utan att det härför uppstår merkostnader eller extra kostnader för uppdragsgivaren.

10.5 Detta uppdragsbehandlingsavtal finns i 18 språkversioner, där den tyska originallydelsen har företräde vid avvikelser.

10.6 Detta avtal är underordnat Bundesrepublik Deutschlands rätt under uteslutning av FNs köprätt. Exklusiv behörighet är München.

10.7 Följande bilagor är avtalets beståndsdelar:

Bilaga 1 - Beskrivning av uppdragsbehandlingen
Bilaga 2 - Tekniska och organisatoriska åtgärder

BILAGA 1 - Beskrivning av uppdragsdatabehandlingen

1 Huvudavtal

Huvudavtal enligt nummer 2.1 i avtalets huvuddel är de ”Allmänna förutsättningar för plattform-användning”.

Titel/Parter: **TB Digital Services GmbH**, Oskar Schlemmer-Strasse 19 - 21, D-80807 München / **Användare**

2 Föremål och uppdragets längd

Uppdragets föremål framgår ur nummer 1 (föremål) och nummer 8 (Användarens data och dataskydd) i huvudavtalet, uppdragets längd framgår ur nummer 7 (Avtalsslut, avtalslängd och uppsägningsrätt) i huvudavtalet.

3 Omfattning, art och ändamål av databehandling/databehandlingsåtgärder

Omfattning, art och ändamål för behandlingen av personuppgifter framgår ur nummer 8 i huvudavtalet.

Närmare beskrivning av uppdragets föremål med hänseende till omfattning, art och ändamål:

För att utföra de av uppdragstagaren erbjudna tjänsterna (som definierats i huvudavtalet), ska uppdragstagaren i för fullgörandet av tjänsterna erforderlig utsträckning samla in personuppgifter från uppdragsgivaren via Connected Vehicles eller Mobile Devices (och eventuellt överförda personuppgifter från en tredjepart med vilken användaren har överenskommit om externa tjänster), överföra dem till uppdragstagarens plattform och spara dem där. Uppdragstagaren ska behandla på plattformen sparade data, i för för fullgörandet av tjänsten nödvändig omfattning,(till exempel för att med hjälp av personuppgifter analysera och utvärdera chaufförernas körsätt, liksom användningen av Connected Vehicle eller Mobile Device och presentera uppdragsgivaren på detta baserade, speciellt till honom anpassade erbjudanden som körträning, utrustningsdetaljer, som förslag till effektivitetsvinst). Exakt omfattning, art och ändamål framgår i synnerhet ur de individuella extra avtal som ska avslutas.

4 Kretsen berörda (kategorier berörda personer)

Följande personkretsar berörs av uppdragsbehandlingen:

- **Chaufförer och annan personal** (anställda i uppdragsgivarens eget bolag), t.ex. arbetstagare, personal under utbildning, platssökande, tidigare anställda*;*
- Chaufförer, som inte är medarbetare;
- **Kontaktpersoner** från lastare/urlastare eller uppdragsgivarens övriga affärspartner; och
- **Koncern-medarbetare** (medarbetare från uppdragsgivarens andra bolagsgrupper)

5 Slag av personuppgifter

Uppdragsdatabehandlingen omfattar följande slag av personuppgifter:

- Chaufförens namn och köridenfikationsnummer;
- Fordonsidentifikationsnummer;
- Sätesdata;
- Data till styr- och liggtider;
- Data till körsätt;
- Connected Vehicles tillståndsdata;
- Trailertillståndsdata;
- Tillståndsdata från på- resp. bakmonterad, aggregat och andra fordonsbyggdelar
- Tillståndsdata från eventuellt kopplade IOT-Devices
- Tillståndsdata från Mobile Devices;
- Laddningsdata;
- Uppdragsdata; och
- Kontaktdata till kontaktpersoner från lastare/urlastare eller uppdragsgivarens övriga affärspartner.

6 Dokumenterade direktiv

Uppdragsgivaren instruerar härmed uppdragstagaren att behandla personuppgifterna enligt nummer 8 i huvudavtalet. Detta inkluderar i synnerhet följande behandling:

- Personuppgifterna överförs via Connected Vehicle eller Mobile Device till uppdragstagarens cloud-baserade plattform och sparas där.
- Personuppgifterna ska under detta avtal bara behandlas i den mån det är nödvändigt för att fullgöra huvudavtalet. Nummer 8.3.4 i huvudavtalet påverkas inte.
- Uppdragstagaren får överlämna personuppgifterna till en tredjepartsleverantör (som definierat i huvudavtalet) bara om och i den mån en sådan överföring till tredje part är nödvändig för att denne ska kunna utföra sina tredjepartstjänster (som definierat i huvudavtalet) för uppdragsgivaren.
- Uppdragstagaren ska med ledning av personuppgifterna analysera och utvärdera chaufförernas körsätt samt användningen av Connected Vehicle och presentera uppdragsgivaren på detta baserade, speciellt till honom anpassade erbjudanden, till exempel körträning, utrustningsdetaljer samt förslag till effektivitetshöjning.

7 Orten för behandling

- Tyskland.
- Förenade kungariket; i den mån data till IT-Hosting och/eller IT-Support-ändamål ska behandlas inom den europeiska unionen behandlas, har motsvarande uppdragsdatabehandlingsavtal ingåtts.
- I den mån uppdragstagare för IT-Hosting- och/eller IT Support-ändamål anlitar underentreprenörer utanför den europeiska unionen (se vidare nummer 8 i denna Bilaga 1), ska överlämnandet av personuppgifter ske på grundval av mellan uppdragstagaren och underentreprenören överenskomna standardavtalsklausuler/standardiserade dataskyddsbestämmelser för överföring av personuppgifter till uppdragsbehandlare i tredjeländer enligt artikel 46.2c GDPR.

8 Underentreprenörer

Uppdragstagaren tillsätter följande underentreprenörer (som eventuellt kan tillsätta ytterligare underuppdragstagare):

Nr.	Underuppdragstagare (firma, adress, kontaktperson)	Behandlade datakategorier	Behandlingssteg/ändamål för underuppdragsdatabehandling
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Samtliga personuppgifter i plattformen, som har att göra med försäljningsdelen (dvs. där en kund kan registrera sig på plattformen och göra beställningar)	Plattform-Hosting
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Samtliga personuppgifter i plattformen, som har att göra med försäljningsdelen (dvs. där en kund kan registrera sig på plattformen och göra beställningar)	IT Support för plattform
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 USA https://aws.amazon.com/de/compliance/contact/	Samtliga övriga personrelaterade användardata som överförs från fordonet till uppdragstagaren	Plattform-Hosting/IT-Support för Plattform-Hosting
4	Vid behov i framtiden i stället för Nr. 3: Amazon Webservices(EU)., Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 USA https://aws.amazon.com/de/compliance/contact/	Samtliga övriga personrelaterade användardata som överförs från fordonet till uppdragstagaren	Plattform-Hosting

5	MAN Service und Support GmbH Dachauer Strasse 667 80995 München, Tyskland Tyskland	Samtliga personrelaterade data som behövs för behandlingen av kundförfrågningar inom ramen för 1st och 2nd Level Support	1st Level Support
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 USA	Samtliga personrelaterade data som behövs för behandling av fakturering/uppdragsgenomförande	Plattform-Hosting (EU Tenant – Gehosted by Amazon Web Services (EU) – se nummer 4
7	MAN Truck & Bus AG Dachauer Str. 667 80995 München, Tyskland Tyskland	Samtliga övriga personrelaterade användardata som överförs till uppdragstagaren via Connected Vehicle och/eller Mobile Device	Plattform-Hosting
8	T-Systems International GmbH Hahnstrasse 43 D-60528 Frankfurt am Main Tyskland	Samtliga övriga personrelaterade användardata som överförs uppdragstagaren via TBM1/2-fordonet	Plattform-Hosting
9	Scania AB Vagnmakarvägen 1 S - 151 87 Södertälje Sweden	Samtliga övriga personrelaterade användardata som överförs från fordonet till uppdragstagaren	Plattform-Hosting
10	Volkswagen Nutzfahrzeuge Mecklenheidestrasse 74 D-30419 Hannover Tyskland	Samtliga övriga personrelaterade användardata som överförs från fordonet till uppdragstagaren	Plattform-Hosting

BILAGA 2 - Tekniska och organisatoriska åtgärder
Tekniska och organisatoriska åtgärder som ska träffas av uppdragstagaren, för att garantera en för risken anpassad skyddsnivå, beskrivs i dataskyddskonceptet till RIO Plattformen och inkluderar särskilt:

1. Pseudonymisering

Såvitt personliga data används för utvärderingsändamål, som även är genomförbar med pseudonymiserade data, används pseudonymiseringsteknik. Därvid definieras tills vidare varje datafält i förväg, om det ska pseudonymiseras, eftersom det skulle möjliggöra en slutsats på en person. Pseudonymiseringsnycklar lagras i en ”Data Safe“, för vilken en maximal åtkomstbegränsning inrättas.

2. Kodning

De mobila terminaler kommunicerar kodat med terminalen med hjälp av ett enhetscertifikat för individuella enheter. Data vidarebefordras kodad inom RIO Plattformen („Ubiquitous encryption“ eller „encryption everywhere“).

3. Sekretessgaranti

Alla medarbetare är och blir hänvisade till sin tystnadsplikt och skriftligt bunden till tysthetsplikten.

Den IT-infrastruktur som används kommer att tillhandahållas av Amazon Web Services (i det följande AWS) inom ramen för en cloud (IaaS & PaaS). Tillträdeskontrollen ställer AWS Data-Center till driftansvarigs förfogande: De högsäkra AWS-Datacenter använder elektroniska övervakningsåtgärder på dagens tillgängliga teknik och flersteg åtkomstkontrollsystem. Datacenter är bemannade dygnet runt med utbildad säkerhetspersonal, och åtkomsten sker strikt på grundval av principer om lägsta behörigheter och beviljas uteslutande för systemadministrationsändamål.

Tillträde till maskinvarukomponenter (Clients) hos TB Digital Services GmbH sker enligt gällande, vid varje enskilt fall tillämpliga standard-åtgärder. Detta är, t. ex., tillträdesinskränkningar genom gripanläggningar (vändkors), videoövervakningsanläggningar, alarmanläggningar och/eller vakttjänst, elektroniskt eller mekaniskt säkrade dörrar, inbrottssäkra byggnader, dokumenterade tillträdesbehöriga (besökare, utomstående) eller deklarerade säkerhetsområden.

Åtkomstkontroller omfattar åtgärder för redskapssäkring, nätverkssäkring och användningssäkring.

Som åtgärder för redskapssäkring i fordon vidtas olika åtgärder: De mobila terminalerna är fast inbyggda i fordonet och förfogar över Secure Boot, dvs. det finns ingen möjlighet att ladda och starta ett främmande operativsystem. De mobila terminalerna kommunicerar kodat med terminalen med hjälp av ett enhetscertifikat för individuella enheter. Data vidarebefordras kodad inom RIO Plattformen („Ubiquitous encryption eller „encryption everywhere“). Terminalerna är genom regelbunden inspelning av säkerhetsuppdateringar på aktuell säkerhetsnivå (Patch-Management).

Som åtgärder för nätverkssäkring vidtas likaså olika standardåtgärder: Det är lämpliga (motsvarande dagens teknik) riktlinjer för lösenord implementerad (lösenordets längd, -komplexitet, -giltighetslängd, osv.). Återkommande felaktig inmatning av användar-id/lösenord-kombination leder till (temporär) avstängning av användar-id. Företagsnätverket är avskärmat genom en Firewall gentemot osäkra öppna nätverk. En process har etablerats, som säkerställer den regelbundna försörjningen av mobila utrustningar med säkerhetsuppdateringar (OTA - Process). För att upptäcka resp. förhindra angrepp på företagsnätverket (Intranet) sätts lämpliga teknologier in (t.ex. Intrusion Detection Systeme). Medarbetarna sensibiliseras regelbundet gällande faror och risker.

Som åtgärder för användningssäkring vidtas några standardåtgärder:

De relevanta användningar är säkrade genom lämpliga autentiserings- och autoriseringsmekanismer mot obehörig åtkomst. Det är lämpliga (motsvarande dagens teknik) riktlinjer för lösenord implementerad (lösenordets längd, -komplexitet, -giltighetslängd, osv.). För användning med särskilda skyddsbehov används starka autentiseringsmekanismer (t.ex. Token, PKI). Återkommande felaktig inmatning av användar-id/lösenord-kombination leder till (temporär) avstängning av användar-id. De i relevanta förfaranden använda data ligger i kodad form på en mobil använd databärare. Genomförda tillträden och åtkomstförsök till användningarna protokollförs. Framtagna loggfiler lagras och kontrolleras (stickprovsmässigt) under en lämplig tidsperiod (minst 90 dagar).

Användarbehöriga (för tillträde och åtkomst) säkerställs med olika åtgärder, där dessa principiellt tilldelas en identifierbar person. Tilldelningen av behöriga ligger i plattform-ansvarigs ansvarighet och kontrolleras regelbundet. Utnämning av åtkomstbehöriga sker endast efter en definierad och dokumenterad process. Ändringar på åtkomstbehöriga sker enligt fyra-ögon-principen och dokumenteras i en versionerad logfile.

Som åtgärd till åtkomstkontroll resp. -styrning vidtas varierande åtgärder: Åtkomsträtten definieras inom ramen för ett roll-/behörighetskoncept, dokumenteras och är motsvarande uppgiftsbetingade krav tilldelad respektive roll. Det är specifika roller/behörigheter för tekniska administratörer inrättad (som, såvitt möjligt, ingen åtkomst på personuppgifter möjliggör). Det är specifika roller/behörigheter för fackmannamässig support inrättad (som inte innehåller några tekniska administratörsrättigheter).

Definitionen av roller/behörigheter och tilldelning av roller/behörigheter sker, såvitt tekniskt och organisatoriskt möjligt, inte genom samma personer och i ett revisionssäkert (tillstånds-)förfarande och är tidsmässigt begränsad. Direkt databasåtkomst, under negligering av roll-/behörighetskonceptet, är enbart genom auktoriserade databasadministratörer möjligt. Det finns en reglering för insats av privata databärare resp. den insatsen av privata databärare är inte tillåten. Det föreligger rättsligt bindande regleringar gällande dataåtkomst vid externa underhåll, fjärrunderhåll och distansarbete. Det görs en integritetsvänlig förstöring/deponering av dokument och databärare (t.ex. Shredder, dataskyddstunna) genom tillförlitliga avfallshanteringsföretag.

Roll-/behörighetskonceptet anpassas regelbundet till ändrade arbetsorganisatoriska strukturer (t.ex. nya roller) och de tilldelade rollerna/behörigheterna kontrolleras regelbundet (t.ex. genom överordnade) och justeras eller

dras in vid behov. En regelbunden central kontroll äger rum gällande tilldelade standardprofiler. De föränderliga åtkomsterna (skrivning, radering) protokollförs och alstrade protokollfiler sparas under ör en lämplig tidsperiod (minst 90 dagar) och kontrolleras (stickprovsmässigt).

Som allmänna åtgärder för att säkra förmedling vidtas olika standardåtgärder:

De med överföringen anlitade personer får i förväg göra sig bekant med säkerhetsåtgärder. Mottagarkretsen definieras i förväg, så att en motsvarande kontroll (autentisering) är möjlig. Den totala processen för dataöverföringen är definierad och dokumenterad och genomförandet av den konkreta dataöverföringen protokollförs resp. dokumenteras (t.ex. mottagningsbevis, kvitto). De med överföringen anlitade personer genomför i förväg en validitets-, fullständighets- och noggrannhetskontroll.

Före genomförandet av den konkreta dataöverföringen görs en översyn av mottagar-adressen (t.ex. Email-adressen). Överföringen av data över Internet sker i kodad form (t.ex.logfilkodning). Integriteten av överförd data blir, såvitt tekniskt möjligt, genom insatsen av signatur-förfaranden (digital signatur) garanterad. Elektroniska mottagningsbevis arkiveras i lämplig form. Oönskade dataöverföringar på Internet hindras genom lämpliga teknologier (t.ex. Proxy, Firewall).

Dessutom kommer som åtgärd för genomförande av separationsbud vidtas följande standardåtgärder:

Det föreligger rättsligt bindande regleringar gällande öronmärkning av behandlingen att separationsbudet efterlevs. De för särskilda ändamål utpekade data lagras separat från data med andra ändamål. Insatta IT-system tillåter separat lagring av data (genom klientresurs eller åtkomstkoncept). Det sker en separation av data i test- och produktivitetssystemer. Vid pseudonymiserade data kommer nyckelbron, som möjliggör en re-identifierbarhet, att lagras separat resp. sparas. Vid uppdragsdatabehandling eller funktionsöverföring ska en separat behandling av data från olika uppdragsgivare ske hos uppdragstagaren. Tillgängliga roll-/behörighetskoncept möjliggör genom sin design den logiska separationen av behandlade data.

4. Integritetsgaranti

Som åtgärder för genomförandet av inmatningsloggning vidtas olika standardåtgärder:

Ändringar av åtkomsträtt, liksom samtliga administrativa tjänster kommer att protokollföras. Skriftliga åtkomster (inmatning, ändringar, raderingar) och förändringar av datafält protokollförs (t.ex. innehållet av nyligen inmatad eller ändrad datapost). Det sker en loggning av överföringar (t.ex. Download) och en login-loggning.

Använt indataunderlag kommer för att kunna följa inmatningar, dokumenteras och arkiveras. Loggningen sker med datum och klockslag, användare, aktivitetens art, användningsprogram och ordningsnummer av dataposten. Loggingsinställningar dokumenteras.

Det beviljas uteslutande läsbar åtkomst på logfiler. Kretsen åtkomstbehöriga av logfiler är snävt begränsad (t.ex. på administratören, dataskyddskommissionären, revisorn). Logfilerna kommer att sparas för en fastlagd tidsperiod (t.ex. 1 år) och raderas sedan integritetsvänlig. Logfilerna kommer regelbundet automatiserat att utvärderas. Utvärderingen av logfiler kommer, såvitt möjligt, att tas fram i pseudonymiserad form.

5. Tillgänglighetsgaranti

Arkitekturen är genom interna repliceringsmekanismer inom AWS Plattformen per se säkrad mot dataförlust. Dessutom vidtas som objektsäkringsåtgärder efterföljande AWS standardåtgärder:

Det vidtas brandskyddsåtgärder (t.ex. brandskyddsdörrar, rökdetektorer, brandskyddsväggar, rökförbud). Dataanläggningar är skyddade mot översvämningar (t.ex. datarummet på första våning, vattendetektor). Det vidtas åtgärder mot skakningar (t.ex. datarummet inte i närheten av genomfartsvägar, tågräls, maskinrum). Dataanläggningar är säkrade mot elektromagnetiska fält (t.ex. stålplattor i ytterväggar). Det vidtas åtgärder mot vandalism och stöld (jfr. tillträdeskontroll). Dataanläggningar finns i luftkonditionerade utrymmen (temperatur och luftfuktighet regleras genom klimatanläggning). Dataanläggningar är säkrade med ett överspännningsskydd mot överspänningstoppar. Det genomförs åtgärder för att säkerställa störningsreducerad och kontinuerlig strömförsörjning (t.ex. UPS-redskap, reservströmaggregat).

Datamängden säkras regelbundet i form av backup-kopior inom AWS Plattformen. Backup-konceptet är dokumenterad och kontrolleras regelbundet och aktualiseras. Backup-medier är skyddade mot obehörig åtkomst. Insatta backup-program motsvarar aktuella kvalitetsstandard och vad detta gäller, regelbundet aktualiserad. Ett redundans-datacenter (tagen från behandlingsorten) har installerats och kan vid katastrofer fortsätta databehandlingen. Olika åtgärder för tillgänglighetskontroll är dokumenterade i en krishanterings-plan av AWS.

Innan ett uppdrag lämnas ut för databehandling, kontrolleras uppdragstagaren noggrant och enligt fasta kriterier (tekniska och organisatoriska åtgärder). Härtill begärs särskild en detaljerad redovisning av från uppdragstagaren genomförda tekniska/organisatoriska dataskyddsåtgärder (svar, frågekatalog eller dataskyddsansvarige) och kontrolleras. Beroende på mängd och sensibilitet av behandlad data sker denna kontroll vid behov även på plats hos uppdragstagaren. Lämplig certifiering (t.ex. ISO 27001) tas hänsyn till vid val av uppdragstagare. Fastställande av uppdragstagarens lämplighet dokumenteras i rimlig och förståelig form.

Som underlag för uppdrags förhållandet ska ett uppdragsdatabehandlingsavtal ingås mellan uppdragsgivaren och uppdragstagaren. Den föreskriver detaljerad och skriftligt behörighet och ansvarighet, liksom båda parters förpliktelser. Om en anlitad tjänsteleverantör har sitt säte utanför EU resp. EWR, används EU-standardavtalsklausulen. Det är reglerat i avtal, att databehandlingen genom uppdragstagaren enbart får ske inom ramen för direktiven från uppdragsgivaren. Uppdragstagaren förpliktas, att omgående redogöra för uppdragsgivaren, om en av hans direktiv enligt uppdragstagarens åsikt bryter mot dataskyddets föreskrifter. För att tillvarata berörda personers rättigheter ska det i uppdragsbehandlingsavtalet överenskommas att

uppdragstagaren på lämpligt sätt ska stödja uppdragsgivaren i den mån detta är nödvändigt t.ex. vid lämnande av upplysningar till berörda personer.

Under den fortsatta uppdragsdatabehandlingen ska uppdragsgivaren kontrollera uppdragstagarens arbetsresultat formellt och innehållsmässigt. Efterlevnad av hos uppdragstagaren träffade tekniska och organisatoriska åtgärder kontrolleras regelbundet. För detta används särskilt förlagan från aktuella attesteringar eller lämpliga certifieringar resp. bevismaterial av genomförda IT-säkerhets- eller dataskyddsrevisioner. Såvitt underentreprenörer tillsätts, är det i avtal bestämt, att dessa motsvarande kontrolleras.

6. Garanti för systemens belastbarhet

AWS Cloud-Infrastrukturen skapades som en av de mest flexibla och säkraste Cloud Computing-Omgivningar. Den koncipierades för ett optimum av tillgänglighet vid fullständig kundseparation. Den levererar en extrem skalbar, ytterst driftsäker plattform, som tillåter kunderna, att globalt snabbt och säkert sprida innehåll vid behov. AWS-Servicen är såtillvida oavhängigt gällande innehåll eftersom de erbjuder samma höga säkerhetsnivå till alla kunder, oberoende av innehållets art eller geografisk region, i vilken innehållen lagras.

De högsäkra AWS-datacenter på världsklassnivå använder elektroniska övervakningsåtgärder med bästa tillgängliga teknik och flersteg åtkomstkontrollsystem. Datacenter är bemannade dygnet runt med utbildad säkerhetspersonal, och åtkomsten sker strikt på grundval av principer om lägsta behörigheter och beviljas uteslutande för systemadministrationsändamål.

7. Förfarande till återställning av tillgänglighet av personuppgifter efter en fysisk eller teknisk incident

AWS-Datacenter uppförs i kluster i olika regioner i världen. Alla datacenter är online och betjänar kunder, inget datacentrum är frånkopplat. Vid ett bortfall flyttar automatiska processer kunddatatrafiken bort från berörda områden. Kärnanvändningar ställs i en N+1-konfiguration till förfogande, så att i händelse av ett bortfall i datacentrum tillräcklig kapacitet finns tillgänglig, för att fördela datatrafiken belastningsfördelad till återstående platser.

AWS erbjuder flexibiliteten att spara, instanser att placera och data inom flera geografiska regioner, liksom över flera Availability Zones, inom enskilda regioner. Varje Availability Zone utvecklades som oavhängig utfallszon. Detta betyder, att Availability Zones inom en typisk stadsregion är fysiskt uppdelad och t.ex. befinner sig i områden med lägre översvämningsrisk (allt efter region finns varierande översvämningszonkategoriseringar). Kompletterande till en självständig avbrottsfri strömförsörjning och reservgeneratorer på plats kommer alla Availability Zones via olika elnät att matas av oberoende elleverantörer, för att minimera punktfelställen. Samtliga Availability Zones är redundans med flera Tier-1-Transit-Provider sammankopplade.

Amazon-Teamet för förvaltning av händelser använder branschvanliga diagnostiska förfaranden, för att snabbare nå en förbättring av företagskritiska händelser. Företagspersonalen erbjuder kontinuerlig närvaro dygnet runt, sju dagar i veckan och 365 dagar per år, för att känna igen driftstörningar och sköta dess följder och förbättring.

8. Förfarande regelbundna kontroller, ändamålsenlighet av tekniska och organisatoriska åtgärder

De riktlinjer och instruktioner som finns I företaget resp. implementerade standarder för informationssäkerhet ska också tillämpas med avseende på införandet och driften av RIO-plattformen. Produktionsfunktioner för dataskydd och informationssäkerhet är tillgängliga (Dataskyddskommissionär och Information Security Officer) De anställda binds till tystnadsplikten och blir informerade via datasäkerhets- resp. IT-säkerhetsåtgärder genom broschyrer, reklamblad, Intranet-riktlinjer osv.

Interna processer kontrolleras med avseende på efterlevnad av tekniska och organisatoriska åtgärder för datasäkerhet genom revision, informationssäkerhet och dataskydd.

Behandlingsförfarande och datasäkerhetsåtgärder dokumenteras i en förteckning över behandlingsverksamhet. Regelbundna kontroller äger rum (internt och externt) över ändamålsenlighet av åtgärderna.