Databehandleravtale
(i henhold til art. 28 DS-GVO)

mellom

brukeren (som definert i hovedkontrakten)

(heretter kalt «**oppdragsgiver**»)

og

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

(heretter kalt «**oppdragstaker**»)
(oppdragsgiveren og oppdragstakeren heretter hver en «**part**» og sammen «**partene**»).

Innledning

(A) Denne databehandleravtalen (heretter «**kontrakt**») anvendes ved alle aktiviteter der oppdragstakeren kommer i kontakt med personopplysninger (som definert i punkt 1.5 nedenfor) fra oppdragsgiveren, fra tredje tilbyder eller andre berørte, i forbindelse med aktiviteten beskrevet i punkt 2 i de generelle rammebetingelsene om bruken av plattformen og ev. enkeltkontrakter, inngått derunder, om ytterligere tjenester (heretter «**hovedkontrakt**»).

(B) I henhold til denne kontrakten handler oppdragsgiveren som behandlingsansvarlig, og oppdragstakeren som databehandler innenfor rammen av et databehandleroppdrag i henhold til art. 28 DS-GVO (som definert nedenfor).

Partene avtaler derfor som følger:

1 Definisjon og interpretasjon

1.1 «**Europisk rett**» er Den europeiske unionens rettsanvendelse, lovanvendelsene til Den europeiske unionens aktuelle medlemsstater og lovanvendelsene til enhver stat som i ettertid blir en medlemsstat av Den europeiske unionen.

1.2 «**Europeisk personvernlovgivning**» er Den europeiske unionens rettsanvendelse ved behandling av personopplysninger (særlig DS-GVO), lov til anvendelsene for Den europeiske unionens aktuelle medlemsstater om personopplysninger (særlig BDSG i den til enhver til gjeldende versjon) og lovanvendelsene ved behandling av personopplysninger til enhver stat som i ettertid blir en medlemsstat i Den europeiske unionen.

1.3 «**DS-GVO**» er «EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om beskyttelse av individer ved behandling av personopplysninger og om fri flyt av slike opplysninger og om oppheving av direktiv 95/46/EF (generell personvernforordning)».

1.4 «**BDSG**» er den tyske personvernforordningen.

1.5 «**Personopplysninger**» har betydningen som definert i BDSG/DS-GVO.

2 Databehandlingens gjenstand / oppdragsgiverens plikter

2.1 Denne kontrakten regulerer partenes forpliktelser i forbindelse med behandlingen av oppdragsgiverens personopplysninger gjennom oppdragstakeren innenfor rammen av hovedkontrakten nevnt i vedlegg 1.

2.2 Behandlingens gjenstand og varighet, behandlingens art og formål, personopplysningenes type, de berørte personenes kategorier og de ansvarliges plikter og rettigheter, finnes i vedlegg 1 til denne kontrakten og i hovedkontraktens ytelsesbeskrivelse.

2.3 Oppdragsgiveren vil fortsatt være behandlingsansvarlig i henhold til DS-GVO og garanterer at det er tillatt å behandle de personopplysningene til de aktuelle personene (sjåfører og ev. andre personer). Spesielt oppfyller oppdragsgiveren sin omfattende informasjonsplikt og sikrer at behandling av personopplysninger er basert på et behandlingsgrunnlag i samsvar med personvernlovgivningen (f.eks. avslutning av en bedriftsavtale, begrensning av behandlingen til formål relatert til ansettelsesforholdet).

3 Oppdragstakerens plikter

3.1 Oppdragstakeren behandler oppdragsgiverens personopplysninger kun til formålene nevnt i vedlegg 1, og innenfor rammen av hovedkontrakten samt i oppdrag og i henhold til de dokumenterte påleggene fra oppdragsgiveren nevnt i vedlegg 1; oppdragstakeren behandler personopplysningene i henhold til denne kontrakten til ingen andre formål. Behandlingen utenfor denne kontrakten til egne formål i henhold til hovedkontraktens siffer 8.3.4, berøres ikke av det. Kopier og duplikater av personopplysninger lages ikke uten oppdragsgiverens viten. Unntak fra dette er sikkerhetskopier i det omfang de er nødvendige for å garantere en forskriftsmessig databehandling, samt data som er nødvendige med hensyn til å overholde lovpålagte oppbevaringsplikter.

3.2 Etter avslutning av oppfyllelsen av behandlingsytelsen må oppdragstakeren etter oppdragsgiverens valg enten overlevere alle personopplysninger fra oppdragsgiveren til oppdragsgiveren og/eller slette disse hos seg selv i henhold til datavernet i det omfang lovpålagte oppbevaringsfrister i henhold til europeisk lovgivning ikke er til hinder for det, og i det omfang oppdragstakeren ikke behandler disse til egne formål utenfor denne kontrakten i henhold til hovedkontraktens punkt 8.3.4. Det samme gjelder test- og avfallsmateriale. Den fullstendige slettingen hhv. utleveringen av dataene til oppdragsgiveren må på forlangende bekreftes skriftlig og med datoangivelse overfor ham.

3.3 I den grad det dekkes av omfanget av tjenesten, støtter oppdragstakeren oppdragsgiveren i oppfyllelsen av de registrertes rettigheter (informasjon, rettelse, motsigelse, sletting) i henhold til oppdragsgiverens instruksjoner.

3.4 Oppdragstakeren bekrefter at han – i den grad det er rettslig foreskrevet – har oppnevnt en personvernansvarlig i bedriften (jf. § 38 BDSG art. 37 DS-GVO).

3.5 Oppdragstakeren er forpliktet til å informere oppdragsgiveren omgående om resultater fra datatilsynets kontroller, i det omfang disse står i sammenheng med oppdragsgiverens databehandling. Eventuelt konstaterte reklamasjoner skal oppdragstakeren utbedre innen rimelig tid, og meddele dette oppdragsgiveren.

3.6 Databehandlingen gjennom oppdragstakeren og underoppdragstakerne godkjent av oppdragsgiveren, finner utelukkende sted i Forbundsrepublikken Tysklands område, i en medlemsstat i Den europeiske unionen eller i en annen avtalestat i traktaten om Det europeiske økonomiske samarbeidsområde. Enhver forflytning i et annet land (heretter «**tredjeland**») trenger oppdragsgiverens uttrykkelige forhåndsgodkjenning, og må i tillegg kun skje hvis de spesielle forutsetningene for dataeksporter til tredjeland er oppfylt (jf. art. 40 ff. DS-GVO). Til dette er det nødvendig med opplysninger i vedlegg 1 og ytterligere (kontrakts-) dokumenter må ev. legges ved.

3.7 Oppdragstakeren må gjøre medarbeidere som er sysselsatt under gjennomføringen av arbeidene, kjent med personvernbestemmelsene som er avgjørende for dem, og forplikte dem til datakonfidensialitet (jf. art. 28 DS-GVO avsn. 3 b) samt gjennom hensiktsmessige tiltak sikre at de ansatte bare behandler personopplysninger på oppdragsgiverens instruksjoner.

3.8 Oppdragstakeren overvåker regelmessig under hele kontraktstiden at kontraktens datavernrettslige forskrifter og oppdragsgiverens dokumenterte pålegg overholdes. På forlangende må kongtrollresultatene legges frem for oppdragsgiveren, i det omfang disse er relevante for oppdragsgiverens databehandling. Tiltakene for overvåkningen er beskrevet i et personvernkonsept som må legges frem for oppdragsgiveren på forlangende.

3.9 Oppdragstakeren må støtte oppdragsgiveren med tanke på behandlingens art og hvis mulig med egnede tekniske og organisatoriske tiltak for å oppfylle sin plikt til å besvare søknader om å ivareta rettighetene til de berørte personene nevnt i kapittel III DS-GVO. Oppdragsgiveren er ansvarlig for kostnadene som oppstår for oppdragstakeren.

3.10 Oppdragstakeren må støtte oppdragsgiveren med tanke på behandlingens art og opplysningene som han disponerer, under overholdelsen av pliktene nevnt i art. 32 til 36 DS-GVO.

4 Tekniske og organisatoriske tiltak angående datasikkerheten

4.1 Oppdragstakeren skal treffe adekvate tekniske og organisatoriske tiltak for personvern (jf. art. 32 DS-GVO). Oppdragstakeren er særlig forpliktet til å gjennomføre de tekniske og organisatoriske tiltakene som er avtalt i vedlegg 2 til denne kontrakten. I løpet av oppdragsforholdet må oppdragstakeren tilpasse disse tiltakene til den tekniske og organisatoriske videreutviklingen, uten samtidig å senke vernenivået. Vesentlige endringer må avtales i skriftlig form.

4.2 På forespørsel påviser oppdragstakeren for oppdragsgiveren den faktiske overholdelsen av de tekniske og organisatoriske tiltakene.

4.3 Oppdragstakeren er forpliktet til å føre en adekvat dokumentasjon av databehandlingen som oppdragsgiveren kan bruke som bevis for den forskriftsmessige databehandlingen. Beviset kan også føres gjennom en godkjent sertifiseringsprosess i henhold til art. 42 DS-GVO.

5 Underoppdragstaker

5.1 Oppdragstakeren får hermed tillatelsen til å trekke inn underoppdragstakere nevnt i vedlegg 1.

5.2 Dette er en generell tillatelse til å trekke inn ytterligere underoppdragstakere. Oppdragstakeren skal derimot informere oppdragsgiveren om enhver påtenkt endring med hensyn til konsultasjonen eller erstatning av underoppdragstakere; oppdragsgiveren kan nedlegge innsigelse mot de påtenkte endringene. Ikke som underoppdragsforhold i denne regelens forstand må slike tjenester anses som oppdragstakeren benytter seg av hos tredjemenn i form av tilleggstjenester som støtte til oppdragsgjennomføringen. Med dette menes f.eks. telekommunikasjonstjenester, rengjøringspersonale, revisorer eller avfallsbehandling av databærere. Oppdragstakeren er derimot forpliktet til å sørge for adekvate og lovlige kontraktsmessige avtaler samt å iverksette kontrolltiltak for å garantere oppdragsgiverens datavern og datasikkerhet også ved tilleggstjenester som er gitt i oppdrag til andre.

5.3 Benytter oppdragstakeren en underleverandør, må oppdragstakeren garantere at vedkommende i form (i) av en kontrakt som sluttes mellom underleverandøren og oppdragstakeren eller (ii) ytterligere juridiske virkemidler i henhold til Den europeiske personvernlovgivningen, pålegges de samme datavernpliktene som pålegges oppdragstakeren i henhold til denne kontrakten. Derved må oppdragstakeren spesielt garantere at underleverandøren gir tilstrekkelige garantier for at de egnede tekniske og organisatoriske tiltakene gjennomføres, slik at behandlingen av personopplysningene skjer i samsvar med kravene til DS-GVO. Etter oppdragsgiverens skriftlige anmodning skal oppdragstakeren gi informasjon til oppdragsgiveren om det vesentlige kontraktsinnholdet og gjennomføringen av forpliktelsene som er relevante for personvernet i underoppdragsforholdet, om nødvendig ved innsyn i de relevante kontraktsdokumentene. Oppdragstakeren har her lov til å sladde kommersielle betingelser. Oppdragsgiveren er forpliktet til hemmeligholdelse av de mottatte opplysningene.

6 Kontrollrettigheter

6.1 Oppdragsgiveren har rett til selv eller gjennom en egnet tredjemann oppnevnt av oppdragsgiveren, å kontrollere hhv. la kontrollere overholdelsen av forpliktelsene i denne kontrakten (inkludert gitte pålegg).

6.2 Oppdragstakeren støtter oppdragsgiveren under kontrollene på en adekvat måte. Spesielt gir oppdragstakeren adgang til databehandlingsanlegg og gir de nødvendige opplysningene.

6.3 I tilfelle en kontroll medfører at oppdragstakeren og/eller behandlingen ikke overholder kontraktens og/eller Den europeiske personvernlovgivningens pålegg, skal oppdragstakeren gjennomføre samtlige korrekturtiltak som er nødvendige for å garantere overholdelsen av instruksjonene til denne kontrakten og/eller til Den europeiske personvernlovgivningen.

6.4 Kostnadene som oppstår for oppdragsgiveren i forbindelse med en kontroll, må han bære selv. Kostnadene som oppstår for oppdragstakeren i forbindelse med en kontroll gjennom oppdragsgiveren, kan han kreve av oppdragsgiveren hvis oppdragsgiveren gjennomfører hhv. lar gjennomføre en kontroll oftere enn én gang per kalenderår.

6.5 Kontroller hos oppdragstakeren må varsles i rett tid, og må ikke påvirke forretningsvirksomheten i urimelig grad.

7 Informasjonsplikter

Oppdragstakeren informerer oppdragsgiveren omgående hvis et pålegg gitt av oppdragsgiveren strider etter oppdragstakerens mening mot Den europeiske personvernlovgivningen. Det med rett reklamerte pålegget må ikke følges så lenge det ikke er endret eller uttrykkelig bekreftet av oppdragsgiveren. Oppdragstakeren er ikke forpliktet til en materiell-rettslig kontroll av pålegg.

Oppdragstakeren må omgående informere oppdragsgiveren i passende form når feil eller uregelmessigheter i databehandlingen oppdages eller ved mistanke om personvernkrenkelser (tilsammen heretter en «**hendelse**»). Oppdragsgiveren må dokumentere hendelsen inkludert alle saksforhold, deres følger og samtlige tiltak for rettelsen, og på oppfordring fra oppdragsgiveren formidle disse dokumenterte opplysningene omgående til oppdragsgiveren i skriftlig eller elektronisk form.

8 Ansvar og fritak

8.1 Oppdragstakeren er ansvarlig for skader som ble forårsaket med fullt overlegg og/eller grov uaktsomhet eller av vedkommendes oppfyllelseshjelper. For skader som beror på oppdragstakerens eller hans oppfyllelseshjelpers enkle uaktsomhet, er oppdragstakeren kun ansvarlig ved brudd på en kardinalplikt. Kardinalplikter er vesentlige kontraktsplikter som først muliggjør en ordentlig gjennomførbarhet av

kontrakten, og hvis oppfyllelse oppdragsgiveren har stolt på og kunne stole på. Ved simpel uaktsomhet angående brudd på slike kardinalplikter er oppdragstakerens ansvar begrenset til skadene som typisk kan forutses.

8.2 Oppdragsgiveren fritar oppdragstakeren fra samtlige krav fra tredjemenn (inkludert berørte personer og/eller personvernmyndigheter), skader og utgifter som beror på oppdragsgiverens brudd på denne kontraktens bestemmelser og/eller på Den europeiske personvernlovgivningen; dette gjelder ikke hvis oppdragsgiveren ikke er skyld i bruddet eller hvis oppdragstakeren har bidratt til bruddet.

9 Løpetid

Kontraktens løpetid tilsvarer hovedkontraktens løpetid. Med avslutning av hovedkontrakten, uansett årsak, avsluttes denne kontrakten automatisk. Oppsigelsen på grunn av en viktig årsak berøres ikke av dette.

10 Annet

10.1 Oppdragstakerens tjenester i henhold til denne kontrakten utlignes gjennom en refusjonsordning regulert i hovedkontrakten.

10.2 Trues oppdragsgiverens personopplysninger hos oppdragstakeren på grunn av tredjemenns tiltak (for eksempel på grunn av utleggsforretning eller beslag), på grunn av insolvens eller gjeldsforhandlinger eller på grunn av øvrige sammenlignbare hendelser, så må oppdragstakeren omgående informere oppdragsgiveren.

10.3 I tilfelle enkelte bestemmelser i denne kontrakten er eller blir uvirksomme, så berører dette ikke virksomheten av de øvrige bestemmelsene. I tilfelle en klausul blir uvirksom, skal partene, med hensyn til saklighet og økonomi, som reserve avtale en ordning som er orientert på kontraktens formål.

10.4 I tilfelle Storbritannia trer ut av Den europeiske unionen, forplikter oppdragstakeren seg allerede nå til å avslutte alle avtaler og å foreta alle handlinger som er nødvendige for å gjennomføre databehandlingen, som er kontraktsgjenstand, på en personvernrettslig tillatt måte i Storbritannia fra fratredelsestidspunktet. Hvis det ikke foreligger noen positiv rimelighetsavgjørelse fra Den europeiske kommisjonen ved fratredelsestidspunktet, er dette, slik det er i dag, spesielt standard personvernklausuler i henhold til artikkel 46 ledd 2 c) for formidling av personopplysninger til oppdragsbehandlere som er etablert i tredjeland der det ikke garanteres noe tilstrekkelig vernenivå.

Etterkommer oppdragstakeren ikke disse forpliktelsene, er oppdragsgiveren berettiget til å kreve av oppdragstakeren, med virkning fra Storbritannias uttredelse av Den europeiske unionen, at de berørte tjenestene utføres av en tilknyttet bedrift hhv. av en bedriftsdel med varig sete i Den europeiske

unionens område uten at det oppstår merkostnader eller ekstra kostnader for oppdragsgiveren i forbindelse med dette.

10.5 Denne databehandleravtalen finnes i 18 forskjellige språk. I tilfelle avvik har den tyske originalteksten prioritet.

10.6 Denne kontrakten er underlagt loven i Forbundsrepublikken Tyskland med utelukkelse av UN-kjøpsrett. Utelukkende verneting er München.

10.7 Følgende vedlegg er del av kontrakten:

Vedlegg 1 – Beskrivelse av databehandlingen
Vedlegg 2 – Tekniske og organisatoriske tiltak

Vedlegg 1 – Beskrivelse av databehandlingen

1 Hovedkontrakt

Hovedkontrakt med hensyn til kontraktens hoveddel punkt 2.1 er de «Generelle rammebetingelsene om bruken av plattformen».

Tittel/parter: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 München / **bruker**

2 Oppdragets gjenstand og varighet

Oppdragets gjenstand fremgår av siffer 1 (*gjenstand*) og hovedkontraktens siffer 8 (*brukerens data og personvern*); kontraktens varighet fremgår av hovedkontraktens siffer 7 (*kontraktsinngåelse, kontraktsvarighet og oppsigelsesrettigheter*).

3 Omfang, art og formål for databehandlingen/databehandlingstiltakene

Omfang, art og formål for behandlingen av personopplysninger fremgår av punkt 8 i hovedkontrakten.

Nærmere beskrivelse av oppdragsgjenstanden med hensyn til omfang, art og formål:

For å kunne yte tjenestene (som definert i hovedkontrakten) som oppdragstakeren har tilbudt, må oppdragstakeren registrere oppdragsgiverens personopplysninger via Connected Vehicles eller Mobile Devices (og ev. personopplysninger som er overført fra en tredje tilbyder, som brukeren har en avtale om tredje tjenester) i den utstrekningen som er nødvendig for ytelsen av tjenestene og overføre til oppdragstakerens plattform og lagre dem der. Oppdragstakeren skal behandle dataene som er lagret på plattformen, i et omfang som er nødvendig for tjenesteytelsen (for eksempel for å analysere og evaluere sjåførenes kjøreegenskaper og bruken av Connected Vehicle eller Mobile Device ved hjelp av personopplysningene, og for å gi oppdragsgiveren, baserende på det, spesielt tilpassede tilbud som for eksempel sjåførtrening, utstyrsdetaljer samt forslag til effektivitetsøkning). Eksakt omfang, art og formål fremgår spesielt av de enkeltkontraktene som må inngås i tillegg.

4 Krets av de berørte (kategorier av berørte personer)

Følgende personkretser er berørt av databehandlingen:

- **Sjåfører og øvrige medarbeidere** (medarbeidere i oppdragsgiverens eget selskap), f.eks. arbeidstagere, lærlinger, jobbsøkere, forhenværende ansatte;
- **Sjåfører** som ikke er medarbeidere;
- **Kontaktpersoner** fra befraktere/avlastere eller oppdragsgiverens øvrige forretningspartnere; og
- **Konsernmedarbeidere** (medarbeidere i et av oppdragsgiverens andre gruppeselskaper).

5 Type personopplysninger

Databehandlingen omfatter følgende typer personopplysninger:

- sjåførens navn og sjåførens identifikasjonsnummer;
- understellsnummer;
- posisjonsdata;
- data om kjøre- og hviletider;
- data om kjøreegenskaper;
- tilstandsdata til Connected Vehicle;
- trailerens tilstandsdata;
- tilstandsdata om overstell hhv. påbygninger, aggregater og ytterligere kjøretøyelementer;
- tilstandsdata for ev. tilkoblede IOT-Devices;
- tilstandsdata for Mobile Devices;
- lastdata;
- oppdragsdata; og
- kontaktdata for kontaktpersoner til befraktere/avlastere eller oppdragsgiverens øvrige forretningspartnere.

6 Dokumenterte pålegg

Oppdragsgiveren gir oppdragstakeren herved pålegg om å behandle personopplysningene som i hovedkontraktens siffer 8. Dette inkluderer spesielt følgende behandling:

- Personopplysningene overføres via Connected Vehicle eller Mobile Device til oppdragstakerens cloud-baserte plattform og lagres der.
- Personopplysningene i denne kontrakten behandles kun i det omfang det er nødvendig for oppfyllelsen av hovedkontrakten; siffer 8.3.4.i hovedkontrakten berøres ikke.
- Oppdragstakeren videreformidler personopplysningene til en tredje tilbyder (som definert i hovedkontrakten), hvis og i det omfang en slik formidling til den tredje tilbyderen er nødvendig for at denne kan yte sine tredje tjenester (som definert i hovedkontrakten) overfor oppdragsgiveren.
- Oppdragstakeren skal ved hjelp av personopplysningene analysere og evaluere sjåførenes kjøreegenskaper og bruken av Connected Vehicle og gi oppdragsgiveren, baserende på det, spesielt tilpassede tilbud som for eksempel sjåførtrening, utstyrsdetaljer samt forslag til effektivitetsøkning.

7 Sted for behandlingen

- Tyskland.
- Storbritannia; hvis det behandles data for IT-hosting og/eller IT-support-formål innen for Den europeiske unionen, ble tilsvarende databehandleravtaler inngått.

- Hvis oppdragstakeren bruker underleverandører utenfor EU for IT-hosting og/eller IT-støtteformål (se punkt 8 i vedlegg 1), vil overføringen av personopplysninger være basert på standard kontraktsbestemmelser/standard personvernbestemmelser inngått mellom oppdragstakeren og underleverandøren for overføring av personopplysninger til databehandlere i tredjeland i henhold til art. 46 Abs. 2 c) DS-GVO.

8 Underoppdragstaker

Oppdragstakeren benytter seg av følgende underoppdragstakere (som ev. kan benytte seg av ytterligere underoppdragstakere):

Nr.	Underoppdragstakere (firma, adresse, kontaktpartner)	Behandlede datakategorier	Behandlingstrinn/formål med databehandlingen av underleverandør
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Samtlige personopplysninger på plattformen som har å gjøre med salgsdelen (dvs. der en kunde kan registrere seg på plattformen og foreta bestillinger)	Plattform-hosting
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Samtlige personopplysninger på plattformen som har å gjøre med salgsdelen (dvs. der en kunde kan registrere seg på plattformen og foreta bestillinger)	IT-support mht. plattform-hosting
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 USA https://aws.amazon.com/de/compliance/contact/	Samtlige øvrige personrelaterte brukerdata som videreformidles via kjøretøyet til oppdragstakeren	Plattform-hosting/IT-support mht. plattform-hosting
4	Ev. i fremtiden i stedet for 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/	Samtlige øvrige personrelaterte brukerdata som videreformidles via kjøretøyet til oppdragstakeren	Plattform-hosting
5	MAN Service und Support GmbH Dachauer Straße 667	Samtlige personopplysninger som er nødvendige for behandlingen av kundeforespørsler innenfor rammen	1st level support

	D-80995 München Tyskland	av 1st og 2nd level support	
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 USA	Samtlige personopplysninger som er nødvendige for behandlingen av faktureringen/oppdragsoppfyllelsen	Plattform-hosting (EU Tenant – hosted by Amazon Web Services (EU) – se siffer 4
7	MAN Truck & Bus AG Dachauer Str. 667 D-80995 München Tyskland	Samtlige øvrige personrelaterte brukerdata som videreformidles via Connected Vehicle og/eller Mobile Device til oppdragstakeren	Plattform-hosting
8	T-Systems International GmbH Hahnstraße 43 D-60528 Frankfurt am Main Tyskland	Samtlige øvrige personrelaterte brukerdata som videreformidles via TBM1/2 kjøretøyet til oppdragstakeren	Plattform-hosting
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Sverige	Samtlige øvrige personrelaterte brukerdata som videreformidles via kjøretøyet til oppdragstakeren	Plattform-hosting
10	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hannover Tyskland	Samtlige øvrige personrelaterte brukerdata som videreformidles via kjøretøyet til oppdragstakeren	Plattform-hosting

VEDLEGG 2 – Tekniske og organisatoriske tiltak
De tekniske og organisatoriske tiltakene som må treffes av oppdragstakeren for å garantere et vernenivå som er tilpasset risikoen, er beskrevet i RIO-plattformens personvernkonseptet, og inkluderer spesielt:

1. Pseudonymisering

I det omfang personopplysningene brukes til evalueringsformål, som også kan gjennomføres med pseudonymiserte data, anvendes pseudonymiseringsteknikker. Her defineres på forhånd for hvert datafelt om det er nødvendig å pseudonymisere, fordi dette ville muliggjøre konklusjoner om en person. Pseudonymiseringsnøklene lagres i en «data-safe» med en så stor tilgangsbegrensning som mulig.

2. Kryptering

De mobile apparatene i hver ende kommuniserer kryptert med hverandre via et apparatindividuelt apparatsertifikat. Innenfor RIO-plattformen videretransporteres dataene kryptert («Ubiquitous encryption» eller «encryption everywhere»).

3. Fortrolighetsgaranti

Alle medarbeidere er og blir informert om deres taushetsforpliktelse, og forpliktes i skriftlig form til datakonfidensialitet.

IT-infrastrukturen som brukes, stilles til disposisjon av Amazon Web Services (heretter AWS) innenfor en cloud (IaaS & PaaS). AWS-Data-Center-operatøren stiller adgangskontrollen til disposisjon: de høysikre AWS-datasentralene bruker elektroniske overvåkningstiltak på teknikkens stand og flertrinns adgangskontrollsystemer. I datasentralene er det hele dagen utdannet sikkerhetspersonale tilstede, og tilgangen tillates strengt etter prinsippet at ingen har rett til tilgang annet enn utelukkende med systemadministrasjon som formål.

Tilgangen til hardwarekomponentene (Clients) hos TB Digital Services GmbH foregår i henhold til gjeldende standard tiltak som er egnet i hvert enkelt tilfelle. Dette er f.eks. adgangsbegrensninger gjennom tilgangskontrollanlegg som tillater kun én person ad gangen (dreiekors), videoovervåkningsanlegg, alarmanlegg og/eller vekterservice, elektronisk eller mekanisk sikrede dører, innbruddssikre bygg, dokumenterte adgangsberettigelser (besøkende, underleverandører) eller deklarerte sikkerhetsområder.

Adgangskontrollene inkluderer tiltak for apparatsikring, nettverkssikring og anvendelsessikring.

Som tiltak for apparatsikringen i kjøretøyet gjennomføres forskjellige tiltak: De mobile sluttapparatene er fast montert i kjøretøyet og har en Secure Boot, dvs. det finnes ingen mulighet for laste og starte et fremmed driftssystem. De mobile apparatene i hver ende kommuniserer kryptert med hverandre via et apparatindividuelt apparatsertifikat. Innenfor RIO-plattformen videretransporteres dataene kryptert («Ubiquitous encryption» eller

«encryption everywhere»). Ved hjelp av regelmessige sikkerhetsoppdateringer er sluttapparatene på et aktuelt sikkerhetsnivå (Patch-Management).

Som tiltak for nettverkssikring gjennomføres også forskjellige standard tiltak: Det er implementert adekvate (i henhold til teknikkens stand) passordtildelinger (passordlengde, -kompleksitet, -gyldighetsvarighet, etc.). Den gjentatte mangelfulle inntastingen av brukeridentifikasjon/passord-kombinasjon medfører en (midlertidig) sperring av brukeridentifikasjonen. Bedriftsnettverket er isolert med en brannmur mot usikre åpne nettverk. Det er etablert en prosess som sikrer den regelmessige forsyningen av mobile apparater med sikkerhetsoppdateringer (OTA – prosess). For å oppdage hhv. unngå angrep på bedriftsnettverket (intranet) anvendes egnede teknologier (f.eks. Intrusion Detection-systemer). Medarbeiderne blir regelmessig sensibilisert mht. farer og risikoer.

Som tiltak for anvendelsessikring gjennomføres forskjellige standard tiltak:

De relevante anvendelsene er sikret med adekvate autentiserings- og autorisasjonsmekanismer mot uvedkommendes tilgang. Det er implementert adekvate (i henhold til teknikkens stand) passordtildelinger (passordlengde, -kompleksitet, -gyldighetsvarighet, etc.). For anvendelser med spesielle vernebehov brukes kraftige autentiseringsmekanismer (f.eks. Token, PKI). Den gjentatte mangelfulle inntastingen av brukeridentifikasjon/passord-kombinasjon medfører en (midlertidig) sperring av brukeridentifikasjonen. Dataene som brukes i den relevante prosessen ligger i kryptert form på en mobil databærer. De gjennomførte tilgangene og tilgangsforsøkene til anvendelsene blir protokollert. De produserte protokollfilene oppbevares i et tjenlig tidsrom (min. 90 dager) og kontrolleres (i form av stikkprøver).

Brukerautorisasjoner (for adgang og tilgang) sikres med forskjellige tiltak som er tilordnet en person som prinsipielt må bestemmes. Tildelingen av autorisasjoner er ansvaret til den plattform-ansvarlige, og kontrolleres regelmessig. Tildelingen av adgangsautorisasjonene gjøres kun i henhold til en definert og dokumentert prosess. Endringer av adgangsautorisasjonene gjøres i henhold til fire-øyne-prinsippet, og dokumenteres i en versjonert loggfil.

Som tiltak for tilgangskontrollen hhv. -styringen gjennomføres forskjellige tiltak: Tilgangsrettighetene defineres og dokumenteres innenfor rammen av et rolle-/berettigelseskonsept, og er tilordnet rollene tilsvarende kravene iht. oppgavene. Det er innrettet spesifikke roller/autorisasjoner for tekniske administratorer (som, hvis teknisk mulig, ikke muliggjør noen tilgang til personopplysninger). Det er innrettet spesifikke roller/autorisasjoner for den faglige supporten (som ikke inneholder noen tekniske administrasjonsrettigheter).

Definisjonen av roller/autorisasjoner og tilordningen av roller/autorisasjoner skjer, så langt teknisk og organisatorisk mulig, ikke gjennom den samme personen og i en revisjonssikker (godkjennings-)prosess, og er tidsbegrenset. Direkte databanktilganger under omgåelse av rolle-/autorisasjonskonseptet, er kun mulig gjennom autoriserte databankadministratorer. Det finnes en regel for bruk av private databærere, dvs. det er forbudt å bruke private databærere. Det foreligger forpliktende regler med hensyn til datatilgang ved ekstern service, fjernservice og telearbeid. Det foretas en personverntilpasset tilintetgjørelse/destruksjon av

dokumenter og databærere (f.eks. shredder, databeskyttelsesbeholdere) gjennom pålitelige renovasjonsselskaper.

Rolle-/autorisasjonskonseptet tilpasses regelmessig til de arbeidsorganisatoriske strukturene som er i endring (f.eks. nye roller), og de tilordnede rolle-/autorisasjonskonseptene kontrolleres regelmessig (f.eks. gjennom de foresatte) og ev. tilpasset hhv. trukket tilbake. Det finner regelmessig sted en sentral kontroll mht. anviste standardprofiler. De tilgangene som er endret (skriving, sletting) protokolleres, og de produserte protokollfilene oppbevares i et tjenlig tidsrom (min. 90 dager) og kontrolleres (i form av stikkprøver).

Som generelle tiltak for sikringen av formidlingen gjennomføres forskjellige standardtiltak:

Personene som er betrodd med formidlingen blir på forhånd gjort fortrolig med sikringstiltak som må treffes. Mottakerkretsen fastsettes på forhånd slik at den tilsvarende kontrollen (autentifisering) er mulig. Den komplette prosessen med dataformidling er fastsatt og dokumentert, og gjennomføringen av den konkrete dataformidlingen protokolleres hhv. dokumenteres (f.eks. mottaksbekreftelse, kvittering). Personene som er betrodd med formidlingen, gjennomfører på forhånd en plausibilitets-, fullstendighets- og riktighetskontroll.

Før den konkrete gjennomføringen av dataoverføringen skjer en kontroll av mottaker-adressen (f.eks. av e-post-adressen). Dataoverføringen via internett skjer i kryptert form (f.eks. som filkryptering). Integriteten av de formidlede dataene blir, hvis teknisk mulig, garantert ved bruk av signatur-prosesser (digital signatur). Elektroniske mottaksbekreftelser arkiveres i egnet form. Uønskede dataoverføringer på internett hindres ved egnede teknologier (f.eks. Proxy, Firewall).

I tillegg gjennomføres som tiltak for gjennomføringen av separasjonskravet, standardtiltakene nedenfor:

Det foreligger forpliktende regler mht. formålsbindingen av behandlingen for overholdelsen av separasjonskravet. Dataene som er registrert for et bestemt formål lagres atskilt fra data som er registrert for andre formål. IT-systemene som benyttes, tillater den atskilte lagringen av data (på grunn av klientkompatibiliteten eller tilgangskonsepter). Det skjer en separasjon av data i test- og produktivsystemer. Ved pseudonymiserte data blir nøkkelen, som muliggjør en reidentifisering, lagret atskilt hhv. oppbevart. Ved databehandling eller funksjonsoverføring skjer en separat databehandling fra forskjellige oppdragsgivere hos oppdragstakeren. De tilgjengelige rolle-/autorisasjonskonseptene muliggjør med sin utforming det logiske skillet av de behandlede dataene.

4. Integritetsgaranti

Som tiltak for gjennomføringen av protokolleringen av inntastingen gjennomføres forskjellige standardtiltak:

Det protokolleres endringer av tilgangsrettighetene samt alle administratoraktiviteter. Det protokolleres skrivende tilganger (inntastinger, endringer, slettinger) og endringer i datafelt (f.eks. innhold av dataposten som er inntastet på nytt eller endret). Det skjer en protokollering av overføringer (f.eks. download) og en loginn-protokollering.

De benyttede registeringsdokumentene blir dokumentert og arkivert for forståelsen av inntastingene. Protokolleringen skjer med dato og klokkeslett, bruker, aktivitetens art, anvendelsesprogrammet og datapostens nummer. Protokolleringsinnstillingene dokumenteres.

Det tillates utelukkende en lesetilgang til protokollfilene. Kretsen av tilgangsberettigede er veldig begrenset (f.eks. til administratoren, den personvernansvarlige, revisoren). Protokollfilene oppbevares i et fastlagt tidsrom (f.eks. 1 år) og slettes deretter i henhold til datavernet. Protokollfilene blir regelmessig evaluert på en automatisert måte. Evalueringer av protokollfilene lages så langt som mulig, i pseudonymisert form.

5. Tilgjengelighetsgaranti

Arkitekturen er sikret per se mot datatap innenfor AWS-plattformen gjennom interne replikeringsmekanismer. I tillegg gjennomføres som tiltak for objektsikringen AWS' standardtiltakene nedenfor:

Det gjennomføres brannverntiltak (f.eks. branndører, røykvarslere, brannmurer, røykeforbud). Dataanleggene er beskyttet mot oversvømmelse (f.eks. datarom i 2. etasje, vannvarsler). Det gjennomføres tiltak mot rystelser (f.eks. datarommet ikke i nærheten av stamvei, togspor, maskinrom). Dataanleggene er sikret mot elektromagnetiske felt (f.eks. stålplater i utvendige vegger). Det gjennomføres tiltak mot vandalisme og tyveri (jf. adgangskontroll). Dataanleggene befinner seg i klimatiserte rom (temperatur og luftfuktighet reguleres via et klimaanlegg). Dataanleggene er sikret med et overspenningsvern mot overspenningsspisser. Det gjennomføres tiltak for å sikre en feilsikker, kontinuerlig strømtilførsel (f.eks. UPS-apparater, nødstrømsaggregater).

De lagrede dataene blir regelmessig sikret i form av backup-kopier innenfor AWS-plattformen. Backup-konseptet er dokumentert og kontrolleres og aktualiseres regelmessig. Backup-mediene er beskyttet mot uautorisert tilgang. Backup-programmene som brukes tilsvarer de aktuelle kvalitetsstandardene, og aktualiseres regelmessig med hensyn til dette. En redundant datasentral (fjernt fra behandlingsstedet) er innrettet og kan fortsette databehandlingen i et katastrofetilfelle. De forskjellige tiltakene for tilgjengelighetskontrollen er dokumentert av AWS i en managementplan for nødstilfeller.

Før tildelingen av et oppdrag om databehandling kontrolleres oppdragstakeren nøye og i henhold til fastsatte kriterier (tekniske og organisatoriske tiltak). Til dette kreves og kontrolleres spesielt en detaljert redegjørelse om tekniske og organisatoriske personverntiltak som oppdragstakeren har gjennomført (besvarelse spørsmålskatalog eller datavernkonsept). Avhengig av mengden og sensibiliteten til de behandlede dataene, gjennomføres denne kontrollen ev. også lokalt hos oppdragstakeren. Egnede sertifiseringer (f.eks. ISO 27001) tas hensyn til ved valg av oppdragstakere. Fastsettelsen av oppdragstakerens egnethet dokumenteres i adekvat og forståelig form.

For stadfestelsen av oppdragsforholdet inngås en databehandleravtale mellom oppdragsgiver og oppdragstaker. Denne fastsetter detaljert og skriftlig begge parters ansvarsområder og ansvar samt plikter. I tilfelle en tjenesteyter har firmasete sitt utenfor EU hhv. EØS, kommer EU-standardkontraktsklausulene til anvendelse. Det er fastsatt i kontrakten at databehandlingen gjennom oppdragstakeren kun må gjennomføres

innenfor rammen av oppdragsgiverens pålegg. Oppdragstakeren blir forpliktet til å opplyse oppdragsgiveren omgående hvis en av dens pålegg, etter oppdragstakerens mening, strider mot personvernets forskrifter. For å oppfylle de berørtes rettigheter, avtales det i databehandleravtalen at oppdragstakeren må støtte oppdragsgiveren i adekvat form, i det omfang dette f.eks. er nødvendig i tilfelle opplysninger meddeles til berørte.

I det videre forløp til databehandlingen kontrollerer oppdragsgiveren oppdragstakerens arbeidsresultater mht. formen og innholdet. Overholdelsen av de tekniske og organisatoriske tiltakene som er truffet hos oppdragstakeren, kontrolleres regelmessig. Til dette brukes frem for alt fremleggelse av aktuelle attester eller egnede sertifiseringer hhv. bevis for gjennomførte IT-sikkerhets- eller personvernkontroller. Hvis det brukes underoppdragstakere, er det bestemt i kontrakten at disse kontrolleres tilsvarende.

6. Garanti for systemenes belastningsevne

AWS Cloud-infrastrukturen ble laget som en av de mest fleksible og sikre Clud Computing-omgivelsene. Den ble konsipert for optimal tilgjengelighet ved fullstendig atskillelse av kundene. Den leverer en ekstrem skalerbar, veldig driftssikker plattform som tillater kundene ved behov å spre innhold raskt og sikkert i hele verden. AWS-Services er uavhengig av innhold ved at de tilbyr alle kundene det samme høye sikkerhetsnivået, uavhengig av innholdets art eller av den geografiske regionen der innholdet lagres.

De høysikre AWS-datasentralene i verdensklassenivå bruker elektroniske overvåkningstiltak på teknikkens stand og flertrinns adgangskontrollsystemer. I datasentralene er det hele dagen utdannet sikkerhetspersonale tilstede, og tilgangen tillates strengt etter prinsippet at ingen har rett til tilgang annet enn utelukkende med systemadministrasjon som formål.

7. Metoder for gjenoppretting av tilgjengeligheten av personopplysninger etter en fysisk eller teknisk hendelse

AWS-datasentraler lages i Clustere i forskjellige regioner i verden. Alle datasentraler er online, og betjener kunder, ingen datasentral er slått av. Ved et utfall skyver automatiske prosesser kundedatatrafikken bort fra de berørte områdene. Kjerneanvendelsene stilles til disposisjon i en N+1-konfigurasjon slik at det finnes tilstrekkelig kapasitet for å fordele datatrafikken lastfordelt til de gjenværende lokaliseringene i tilfelle datasentralen faller ut.

AWS tilbyr fleksibiliteten til å plassere instanser og til å lagre data innenfor flere geografiske regioner og over flere Availability Zones innenfor den enkelte regionen. Hver Availability Zone er utviklet som uavhengig driftsstanssone. Dette betyr at Availability Zones innenfor en typisk byregion er fordelt fysisk og befinner seg i områder med lav oversvømmelsesrisiko (avhengig av regionen finnes kategoriseringer for oversvømmelsessoner). I tillegg til en selvstendig avbrudssfri strømtilførsel og nødstrømsgeneratorer på stedet, blir alle Availability Zones matet via forskjellige strømnett av uavhengige strømleverandører for å minimere enkeltfeilpunkter. Alle Availability Zones er koblet redundant med flere Tier-1-Transit-leverandører.

Amazon-teamet for administrasjon av hendelser bruker diagnostiske metoder som er vanlige i bransjen, for å fremskynde rettingen av bedriftskritiske hendelser. Driftspersonalet er hele dagen kontinuerlig tilgjengelig, sju dager i uken og 365 dager i året, for å oppdage feil og for å administrere deres konsekvenser og retting.

8. Prosesser for virksomhetens regelmessige kontroll, vurdering og evaluering av de tekniske og organisatoriske tiltakene

Bedriftens retningslinjer og anvisninger hhv. de implementerte standardene om informasjonssikkerheten, anvendes også for innføringen og driften av RIO-plattformen. Bedriftsfunksjoner for personvern og informasjonssikkerhet finnes (ansvarlig for personvern og Information Security Officer). De ansatte er forpliktet til å opprettholde datakonfidensialitet, og informeres om datasikkerhets- hhv. IT-sikkerhetstiltak via brosjyrer, flyers, intranet-henvisninger etc.

Når det gjelder overholdelsen av tekniske og organisatoriske tiltak angående datasikkerhet, kontrolleres de interne prosessene via revisjon, informasjonssikkerhet og personvern.

Behandlingsprosessene og datasikkerhetstiltakene dokumenteres i et register for behandlingsaktiviteter. Det gjennomføres regelmessig en kontroll (intern og ekstern) med hensyn til tiltakenes virksomhet.