Ugovor o provođenju obrade (prema članku 28. GDPR-a)

između

Korisnika (kako je definirano u Glavnom ugovoru)

(u nastavku teksta „**Naručitelj**")

i

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

(u nastavku teksta „**Izvođač**")
(Naručitelj i Izvođač u nastavku se pojedinačno navode kao „**ugovorna strana**", odnosno zajedno „**ugovorne strane**").

Preambula

(A) Ovaj Ugovor o provođenju obrade (u nastavku „**Ugovor**") primjenjuje se na sve djelatnosti pri kojima Izvođač dolazi u dodir s osobnim podacima Naručitelja (kako je definirano niže u točki 1.5), trećih strana ili ostalih zainteresiranih strana u vezi s aktivnošću opisanom u točki 2 Općih okvirnih uvjeta za upotrebu platforme i u, ako postoje, pojedinačnim ugovorima o dodatnim uslugama sklopljenima u okviru tih uvjeta (u nastavku „**Glavni ugovor**").

(B) Prema ovome Ugovoru Naručitelj je voditelj obrade, a Izvođač je izvršitelj obrade u okviru ugovorene obrade naloga prema članku 28. GDPR-a (kako je definirano niže).

Ugovorne strane sporazumjele su se kako slijedi:

1 Definicije i tumačenja

1.1 „**Europsko pravo**" primjenjivo je pravo Europske unije, primjenjivi zakoni trenutačnih država članica Europske unije te primjenjivi zakoni svake pojedine države koja naknadno postane država članica Europske unije.

1.2 „**Europsko pravo o zaštiti podataka**" primjenjivo je pravo Europske unije o obradi osobnih podataka (osobito GDPR), primjenjivi zakoni trenutačnih država članica Europske unije o obradi osobnih podataka (osobito BDSG u svojoj trenutačno važećoj inačici) te primjenjivi zakoni svake pojedine države koja naknadno postane država članica Europske unije o obradi osobnih podataka.

1.3 „**GDPR**" je „UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)".

1.4 „**BDSG**" je Savezni zakon o zaštiti podataka.

1.5 „**Osobni podaci**" ima značenje kako je definirano u BDSG-u / GDPR-u.

2 Predmet obrade podataka / obveze Naručitelja

2.1 Ovim Ugovorom uređuju se obveze ugovornih strana u vezi s obradom osobnih podataka Naručitelja koju obavlja Izvođač, u okviru Priloga 1. navedenoga Glavnog ugovora.

2.2 Predmet i trajanje obrade, način i svrha obrade, vrsta osobnih podataka, kategorije uključenih osoba i obveze i prava odgovornih strana proizlaze iz Priloga 1. ovoga Ugovora te specifikacije Glavnog ugovora.

2.3 Naručitelj ostaje voditelj obrade u smislu GDPR-a i jamči da posjeduje dopuštenje za obradu osobnih podataka zainteresiranih strana (vozača i po potrebi ostalih osoba). U tom pogledu Naručitelj posebno ispunjava svoju opsežnu obvezu pružanja informacija i jamči da za obradu osobnih podataka postoji pravni temelj koji je usklađen sa zakonom o zaštiti osobnih podataka (npr. sklapanje ugovora o radovima, ograničavanje obrade na potrebe radnog odnosa).

3 Obveze Izvođača

3.1 Izvođač obrađuje osobne podatke Naručitelja isključivo u svrhe navedene u Prilogu 1. i u okviru Glavnog ugovora, te prema uputama Naručitelja navedenima u narudžbi i dokumentiranima u Prilogu 1.; Izvođač prema ovom Ugovoru ne obrađuje osobne podatke ni u koje druge svrhe. Time se ne dovodi u pitanje obrada za vlastite potrebe izvan primjene ovoga Ugovora prema točki 8.3.4. Glavnog ugovora. Bez znanja Naručitelja ne izrađuju se kopije ni duplikati osobnih podataka. Iz toga su izuzete sigurnosne kopije ukoliko su neophodne za osiguravanje uredne obrade podataka, kao i podaci koji su potrebni za ispunjavanje zakonskih obveza o čuvanju podataka.

3.2 Nakon završetka pružanja usluga obrade Izvođač mora prema izboru Naručitelja sve osobne podatke Naručitelja ili predati i/ili izbrisati sâm u skladu s propisima o zaštiti podataka, ako to nije u suprotnosti s obveznim razdobljem čuvanja podataka i ako ih Izvođač nije obradio za vlastite potrebe izvan primjene ovoga Ugovora prema točki 8.3.4. Glavnog ugovora. Isto vrijedi za testni i otpadni materijal. Potpuno brisanje, odnosno predaja podataka Naručitelju, na zahtjev Naručitelja mora se potvrditi istome u pisanom obliku uz navođenje datuma.

3.3 Ako opseg usluge to obuhvaća, Izvođač će podržati Naručitelja pri ispunjavanju prava ispitanika (pravo na pristup, ispravak, ulaganje prigovora, brisanje) prema odgovarajućoj uputi Naručitelja.

3.4 Izvođač potvrđuje da je – ako je zakonom propisano – imenovao stručnog službenika za zaštitu podataka (usp. članak 38. BDSG-a članak 37. GDPR-a).

3.5 Izvođač se obvezuje da će bez odgode obavijestiti Naručitelja o rezultatu ispitivanja koja provedu tijela nadležna za zaštitu podataka, ako su ona u vezi s obradom podataka Naručitelja. U slučaju utvrđenih nesukladnosti Izvođač će u razumnom roku ukloniti te nesukladnosti i o tome obavijestiti Naručitelja.

3.6 Obrada podataka koju obavljaju Izvođač i podizvođači koje je ovlastio Naručitelj odvija se isključivo u Saveznoj Republici Njemačkoj, u državi članici Europske unije ili u drugoj ugovornoj državi Sporazuma o Europskom gospodarskom prostoru. Za bilo kakvo premještanje u neku drugu zemlju (u nastavku „**treća zemlja**") potrebno je prethodno izričito dopuštenje Naručitelja te smije uslijediti samo ako su ispunjeni posebni uvjeti za izvoz podataka u treće zemlje (usp. članak 40. i naredne članke GDPR-a). Pri tome su obvezni podaci iz Priloga 1., a prema potrebi moraju se priložiti dodatni (ugovorni) dokumenti.

3.7 Prilikom izvođenja radova Izvođač mora upoznati zaposlenike s odredbama o zaštiti podataka koje su mjerodavne za njih i obvezati ih na čuvanje tajnosti podataka (usp. članak 28. stavak 3. točka (b) GDPR-a) te osigurati odgovarajućim mjerama da ti zaposlenici obrađuju osobne podatke samo prema uputi Naručitelja.

3.8 Izvođač redovito tijekom cijelog trajanja Ugovora nadzire pridržavanje zakonskih odredbi o zaštiti podataka iz ovog Ugovora i dokumentiranih uputa Naručitelja. Rezultati kontrola dostavljaju se Naručitelju na zahtjev ako su relevantni za obradu podataka Naručitelja. Mjere za nadzor opisane su u konceptu zaštite podataka koji se na zahtjev dostavlja Naručitelju.

3.9 Uzimajući u obzir prirodu obrade, Izvođač pomaže Naručitelju putem odgovarajućih tehničkih i organizacijskih mjera, koliko je to moguće, da ispuni obvezu voditelja obrade u pogledu odgovaranja na zahtjeve za ostvarivanje prava ispitanika koja su utvrđena u poglavlju III. Naručitelj snosi troškove Izvođača koji pritom nastanu.

3.10 Izvođač, uzimajući u obzir prirodu obrade i informacije koje su mu na raspolaganju, mora pružati podršku Naručitelju da ispuni obveze iz članaka 32. do 36. GDPR-a.

4 Tehničke i organizacijske mjere za zaštitu podataka

4.1 Izvođač provodi odgovarajuće tehničke i organizacijske mjere za zaštitu podataka (usp. članak 32. GDPR-a). Izvođač je osobito obvezan provoditi tehničke i organizacijske mjere utvrđene u Prilogu 2. ovome Ugovoru. Navedene mjere Izvođač tijekom trajanja ugovornog odnosa mora prilagoditi tehničkom i organizacijskom razvoju, a da pritom ne smanji razinu zaštite. Značajne izmjene moraju se dogovoriti pisanim putem.

4.2 Izvođač Naručitelju na upit dokazuje da se stvarno pridržava tehničkih i organizacijskih mjera.

4.3 Izvođač je obvezan voditi odgovarajuću dokumentaciju o obradi podataka na temelju koje Naručitelj može predočiti dokaz o urednoj obradi podataka. Dokaz se može pribaviti i odobrenim mehanizmom certificiranja prema članak 42. GDPR-a.

5 Podizvođač

5.1 Izvođaču se ovime dopušta uključivanje podizvođača navedenih u Prilogu 1.

5.2 Općenito se dopušta uključivanje daljnjih podizvođača. Izvođač obavještava Naručitelja o svim planiranim izmjenama u vezi s dodavanjem ili zamjenom podizvođača; Naručitelj može uložiti prigovor na planirane izmjene. U smislu ove odredbe usluge trećih strana kojima se Izvođač koristi kao sporednim uslugama za podršku pri obavljanju narudžbe ne smatraju se podugovornim odnosom. To uključuje npr. telekomunikacijske usluge, osoblje za čišćenje, ispitivače ili odlaganje nosača podataka. Izvođač i dalje ima obvezu ispunjavanja odgovarajućih ugovornih obveza koje su u skladu sa zakonom te poduzimanja kontrolnih mjera kako bi zajamčio zaštitu i sigurnost podataka Naručitelja čak i u slučaju sporednih usluga koje pružaju treće strane.

5.3 Ako Izvođač angažira podizvođača, mora se pobrinuti da se na podizvođača primjenjuju jednake obveze o zaštiti podataka koje se primjenjuju na Izvođača kako je utvrđeno ovim Ugovorom, ili putem (i) ugovora koji je sklopljen između podizvođača i Izvođača ili (ii) drugog pravnog instrumenta prema europskom pravu u području zaštite podataka. Pritom Izvođač osobito treba osigurati da podizvođač pruža dostatna jamstva za provođenje odgovarajućih tehničkih i organizacijskih mjera kako bi se obrada osobnih podataka provodila prema zahtjevima iz GDPR-a. Na pisani zahtjev Naručitelja Izvođač Naručitelju dostavlja informacije o bitnom sadržaju i ispunjavanju obveza relevantnih za zaštitu podataka koji su utvrđeni u podugovornom odnosu, prema potrebi pružanjem uvida u relevantnu ugovornu dokumentaciju. Izvođač pritom smije zatamniti komercijalne uvjete. Naručitelj je obvezan čuvati povjerljivosti dobivenih informacija.

6 Prava nadzora

6.1 Naručitelj ima pravo samostalno ili preko odgovarajuće treće strane koju je imenovao nadzirati poštuju li se obveze iz ovoga Ugovora (uključujući i upute).

6.2 Izvođač jamči Naručitelju primjerenu podršku u provedbi nadzora, osobito pristup dokumentima o obradi podataka, te pruža potrebne informacije.

6.3 U slučaju da rezultat nadzora pokaže da Izvođač i/ili obrada nije u skladu s odredbama iz ovoga Ugovora i/ili europskog prava u području zaštite podataka, Izvođač poduzima sve potrebne korektivne mjere da bi jamčio pridržavanje odredbi ovoga Ugovora i/ili europskog prava u području zaštite podataka.

6.4 Naručitelj snosi troškove koji nastanu tijekom nadzora koji provodi. Izvođač od Naručitelja može zatražiti da pokrije troškove koji su nastali na strani Izvođača tijekom nadzora koji provodi Naručitelj, ako Naručitelj, odnosno treća strana u ime Naručitelja, provodi taj nadzor više od jedanput u kalendarskoj godini.

6.5 Provedbu nadzora potrebno je pravodobno najaviti Izvođaču i ona ne smije nerazmjerno ometati rad Izvođača.

7 Obveze navođenja informacija

Izvođač bez odgode obavještava Naručitelja ako smatra da je uputa dobivena od Naručitelja u suprotnosti s europskim pravom u području zaštite podataka. Opravdano osporenu uputu ne treba slijediti sve dok je Naručitelj ne izmijeni ili izričito potvrdi. Izvođač nije obvezan materijalno i pravno provjeravati upute.

Obveza je Izvođača da u slučaju utvrđenih grešaka ili nepravilnosti u obradi podataka ili u slučaju sumnje na kršenje odredbi o zaštiti podataka (u nastavku zajednički naziv „**slučaj**"), o tome bez odgode primjereno informira Naručitelja. Naručitelj mora dokumentirati slučaj zajedno sa svim činjeničnim okolnostima, njegovim učincima i svim mjerama za njihovo uklanjanje te na zahtjev Naručitelja bez odgode dostaviti te informacije Naručitelju pisanim ili elektroničkim putem.

8 Odgovornost i izuzeće

8.1 Izvođač odgovara za štetu koju namjerno i/ili krajnjom nepažnjom prouzroči Izvođač ili njegovi zastupnici. Za štetu koja nastane uslijed obične nepažnje Izvođača ili njegovih zastupnika Izvođač odgovara samo ako se radi o povredi glavne ugovorne obveze. Glavne ugovorne obveze ključne su ugovorne obveze koje omogućuju urednu provedbu Ugovora i u čije se ispunjavanje Naručitelj pouzdao i trebao bi se moći pouzdati. U slučaju obične nepažnje u pogledu povrede takvih glavnih ugovornih obveza odgovornost Izvođača ograničena je na uobičajeno predvidljivu štetu.

8.2 Naručitelj ne tereti Izvođača za cjelokupne zahtjeve trećih strana (uključujući osobe na koje se to odnosi i/ili tijela nadležna za zaštitu podataka), odštete i izdatke koji proizlaze iz Naručiteljeva kršenja odredbi ovoga Ugovora i/ili europskoga prava u području zaštite podataka; ova odredba nije primjenjiva ako Naručitelj nije odgovoran za kršenje ili ako je Izvođač pridonio kršenju.

9 Vrijeme rada

Trajanje ovoga Ugovora odgovara trajanju Glavnog ugovora. S raskidom Glavnog ugovora iz bilo kojeg razloga automatski se raskida i ovaj Ugovor. Pravo na raskid iz opravdanog razloga ostaje nepromijenjeno.

10 Ostalo

10.1 Usluge Izvođača prema ovome Ugovoru podmiruju se u skladu s odredbom o naknadi iz Glavnog ugovora.

10.2 Ako su osobni podaci Naručitelja koji se nalaze kod Izvođača ugroženi postupanjem trećih strana (npr. zbog pljenidbe ili oduzimanja), nesolventnošću ili postupkom nagodbe ili drugim usporedivim događajima, Izvođač bez odgode o tome obavještava Naručitelja.

10.3 U slučaju da su pojedine odredbe ovoga Ugovora ništavne ili postanu ništavne, učinkovitost ostalih odredbi ostaje nepromijenjena. U slučaju ništavnosti određene klauzule ugovorne strane dogovaraju njezinu zamjenu odredbom koja u činjeničnom i poslovnom smislu odgovara svrsi ovoga Ugovora.

10.4 Za slučaj izlaska Velike Britanije iz Europske unije Izvođač se već sada obvezuje na zaključivanje svih sporazuma i poduzimanje svih radnji koje su potrebne da se od trenutka izlaska obrada podataka iz predmeta ovog Ugovora u Velikoj Britaniji nastavi provoditi tako da je u skladu sa zakonima o zaštiti podataka. Ako u trenutku izlaska ne postoji odluka Europske komisije o primjerenosti, s današnjega gledišta to su posebice standardne klauzule za zaštitu podataka prema članku 46. stavku 2. točki (c) o prijenosu osobnih podataka izvršiteljima obrade s poslovnim nastanom u trećim zemljama u kojima nije zajamčena primjerena razina zaštite.

Ako Izvođač ne ispuni ove obveze, Naručitelj ima pravo zatražiti od Izvođača da s učinkom od izlaska Velike Britanije iz Europske unije predmetne usluge pruža povezano poduzeće, odnosno dio poduzeća sa stalnim sjedištem na području Europske unije, a da pritom za Naručitelja ne nastane izdatak ili dodatni troškovi.

10.5 Ovaj Ugovor o provođenju obrade dostupan je na 18 jezika, pri čemu u slučaju odstupanja prednost ima njemački izvornik.

10.6 Ovaj Ugovor podliježe pravu Savezne Republike Njemačke, isključujući Konvenciju Ujedinjenih naroda o ugovorima o međunarodnoj prodaji robe. Isključivo mjesto nadležnosti jest München.

10.7 Sljedeći prilozi sastavni su dio Ugovora:

Prilog 1. – opis ugovorenog provođenja obrade
Prilog 2. – tehničke i organizacijske mjere

PRILOG 1. – opis ugovorenog provođenja obrade

1 Glavni ugovor

Glavni ugovor u smislu točke 2.1 glavnog dijela Ugovora jesu „Opći okvirni uvjeti za korištenje platforme".

Titula / Ugovorne strane: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 München / **Korisnik**

2 Predmet i trajanje ugovora

Predmet ugovora proizlazi iz točke 1. (*Predmet*) i točke 8. Glavnog ugovora (*Podaci Korisnika i zaštita podataka*); trajanje ugovora proizlazi iz točke 7. Glavnog ugovora (*Sklapanje ugovora, trajanje ugovora i prava na raskid*).

3 Opseg, priroda i svrha obrade podataka / Mjere za obradu podataka

Opseg, priroda i svrha obrade osobnih podataka proizlaze iz točke 8. Glavnog ugovora.

Pobliži opis predmeta ugovora u pogledu opsega, prirode i svrhe:

da bi Izvođač mogao pružati usluge koje nudi (kako je definirano u Glavnom ugovoru), mora prikupiti osobne podatke Naručitelja putem sustava Connected Vehicles ili Mobile Devices (i prema potrebi osobne podatke prenesene ponuđaču treće strane s kojim je Korisnik ugovorio pružanje usluga) u mjeri potrebnoj za pružanje usluga i prenijeti ih na platformu Izvođača te ih tamo pohraniti. Izvođač će obraditi podatke spremljene na platformi u mjeri potrebnoj za pružanje usluge (npr. da bi na temelju osobnih podataka analizirao i ocijenio ponašanje vozača u vožnji kao i upotrebu sustava Connected Vehicle i Mobile Device te na temelju toga dostavio Naručitelju posebne, za njega prilagođene ponude, kao npr. treninge za vozače, detalje za opremu kao i prijedloge za povećanje učinkovitosti). Točan opseg, priroda i svrha proizlaze osobito iz pojedinačnih ugovora koji se dodatno sklapaju.

4 Zainteresirane strane (kategorije zainteresiranih osoba)

Ugovoreno provođenje obrade odnosi se na sljedeće skupine zainteresiranih osoba:

- **vozači i ostali zaposlenici** (zaposlenici vlastitog poduzeća Naručitelja), npr. posloprimci, pripravnici, kandidati za zaposlenje, nekadašnji zaposlenici*;*
- **vozači** koji nisu zaposlenici;
- **kontaktne osobe** utovarivača/istovarivača ili drugih poslovnih partnera Naručitelja; i
- **zaposlenici koncerna** (zaposlenici drugog poduzeća unutar grupacije Naručitelja).

5 Vrsta osobnih podataka

Ugovoreno provođenje obrade obuhvaća sljedeće vrste osobnih podataka:

- ime vozača i identifikacijski broj vozača
- identifikacijski broj vozila
- podatke o lokaciji
- podatke o trajanju vožnje i mirovanja vozila
- podatke o ponašanju u vožnji
- podatke o statusu sustava Connected Vehicle
- podatke o stanju prikolice
- podatke o stanju nadograđenih i ugrađenih dijelova, agregata i drugih dijelova vozila
- ako postoje, podatke o statusu povezanih IOT uređaja
- podatke o statusu sustava Mobile Devices
- podatke o punjenju
- podatke o nalogu i
- podatke kontaktnih osoba utovarivača/istovarivača ili drugih poslovnih partnera Naručitelja.

6 Dokumentirane upute

Ovim putem Naručitelj nalaže Izvođaču da obradi osobne podatke kao u točki 8. Glavnog ugovora. To osobito uključuje sljedeću obradu:

- Osobni podaci prenose se putem sustava Connected Vehicle ili Mobile Device na platformu u oblaku Izvođača i tamo se pohranjuju.
- Osobni podaci obrađuju se prema ovom Ugovoru samo ako je to neophodno za ispunjavanje Glavnog ugovora; točka 8.3.4. Glavnog ugovora ostaje nepromijenjena.
- Izvođač prenosi osobne podatke trećem ponuđaču (kako je definirano Glavnim ugovorom) ako je takav prijenos trećem ponuđaču neophodan kako bi treći ponuđač mogao pružiti svoje usluge treće strane (kako je definirano Glavnim ugovorom) Naručitelju.
- Izvođač će na temelju osobnih podataka analizirati i ocijeniti ponašanje vozača u vožnji kao i upotrebu sustava Connected Vehicle i Mobile Device te na temelju toga dostaviti Naručitelju posebne, za njega prilagođene ponude, kao npr. treninge za vozače, detalje za opremu kao i prijedloge za povećanje učinkovitosti.

7 Lokacija obrade

- Njemačka.
- Ujedinjena Kraljevina; ako se podaci za IT usluge poslužitelja i/ili svrhe pružanja IT podrške obrađuju u Europskoj uniji, sklopljeni su odgovarajući ugovori o provođenju obrade.

- Ako Izvođač angažira podizvođača izvan Europske unije za IT usluge poslužitelja i/ili svrhe pružanja IT podrške (vidi točku 8. Ovog Priloga 1.), prijenos osobnih podataka obavlja se na temelju standardnih ugovornih klauzula / standardnih klauzula za zaštitu podataka koje su sklopili Podizvođač i Naručitelj o prijenosu osobnih podataka izvršiteljima obrade u trećim zemljama prema članku 46. stavku 2. točki (c) GDPR-a.

8 Podizvođač

Izvođač angažira sljedeće podizvođače (koji prema potrebi mogu angažirati dodatne podizvođače):

Br.	Podizvođač (tvrtka, adresa, kontaktna osoba)	Obrađene kategorije podataka	Koraci obrade / Svrha podugovorenog provođenja obrade
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, SAD	Cjelokupni osobni podaci na platformi koji su povezani s prodajom (tj. gdje se kupac na platformi može registrirati i poslati narudžbe)	Usluge poslužitelja na platformi
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, SAD	Cjelokupni osobni podaci na platformi koji su povezani s prodajom (tj. gdje se kupac na platformi može registrirati i poslati narudžbe)	IT podrška u vezi s platformom
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 SAD https://aws.amazon.com/de/compliance/contact/	Cjelokupni ostali osobni podaci korisnika koji se prenose Izvođaču preko vozila	Usluge poslužitelja na platformi / IT podrška u vezi s platformom
4	Prema potrebi u budućnosti umjesto br. 3: Amazon Webservices (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 SAD https://aws.amazon.com/de/compliance/contact/	Cjelokupni ostali osobni podaci korisnika koji se prenose Izvođaču preko vozila	Usluge poslužitelja na platformi
5	MAN Service und Support GmbH Dachauer Straße 667	Cjelokupni osobni podaci koji su potrebni za obradu upita korisnika u okviru 1. i 2. razine korisničke	1. razina korisničke podrške

	80995 München Njemačka	podrške	
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 SAD	Cjelokupni osobni podaci koji su potrebni za obradu izdavanja računa / isporuku narudžbe	Usluge poslužitelja na platformi (EU Tenant – usluge pohrane podataka na poslužitelju pruža Amazon Web Services (EU) – vidi točku 4.)
7	MAN Truck & Bus AG Dachauer Str. 667 80995 München Njemačka	Cjelokupni ostali osobni podaci korisnika koji se prenose Izvođaču putem sustava Connected Vehicle i/ili Mobile Device	Usluge poslužitelja na platformi
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Njemačka	Cjelokupni ostali osobni podaci korisnika koji se prenose Izvođaču preko vozila TBM1/2	Usluge poslužitelja na platformi
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Švedska	Cjelokupni ostali osobni podaci korisnika koji se prenose Izvođaču preko vozila	Usluge poslužitelja na platformi
10	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hannover Njemačka	Cjelokupni ostali osobni podaci korisnika koji se prenose Izvođaču preko vozila	Usluge poslužitelja na platformi

PRILOG 2. – tehničke i organizacijske mjere
Tehničke i organizacijske mjere koje Izvođač mora poduzeti da bi jamčio razinu zaštite primjerenu riziku opisane su u konceptu zaštite podataka za platformu RIO i uključuju osobito sljedeće stavke:

1. Pseudonimizacija

Ako se osobni podaci upotrebljavaju u svrhe izrade procjena koje se mogu provesti i sa pseudonimiziranim podacima, provodi se pseudonimizacija. Pritom se prvo za svako podatkovno polje unaprijed utvrđuje mora li se pseudonimizirati prema tome bi li omogućilo donošenje zaključka o osobi. Ključevi pseudonimizacije odlažu se u „podatkovni sef" za koji je postavljeno najveće moguće ograničenje pristupa.

2. Šifriranje

Mobilni krajnji uređaji komuniciraju u šifriranom obliku s krajnjom točkom putem certifikata specifičnog za pojedini uređaj. Podaci se dalje u šifriranom obliku prenose unutar platforme RIO („Ubiquitous encryption" ili „encryption everywhere").

3. Jamstvo povjerljivosti

Svi zaposlenici upoznati su i bit će upoznati sa svojom obvezom čuvanja povjerljivosti i obvezani su na čuvanje tajnosti podataka pisanim putem.

IT infrastrukturu za korištenje na raspolaganje stavlja Amazon Web Services (u nastavku AWS) u okviru oblaka (IaaS & PaaS). Kontrolu pristupa na raspolaganje stavlja operator podatkovnog centra AWS-a: u računalnim centrima AWS-a s visokom razinom sigurnosti primjenjuju se elektroničke mjere nadzora najnovijeg stupnja tehničkog razvoja i višerazinske sustave kontrole pristupa. U računalnim centrima u svako doba nalazi se obučeno zaštitarsko osoblje, a pristup se daje prema načelu najmanjih prava i isključivo u svrhe administracije sustava.

Pristup hardverskim komponentama (Clients) tvrtke TB Digital Services GmbH odvija se prema važećim standardnim mjerama koje se primjenjuju za svaki pojedinačni slučaj. To se postiže npr. ograničenjima pristupa putem sustava razdvajanja (križne rampe), sustavom video-nadzora, alarmnim sustavom i/ili službom nadzora, elektronički ili mehanički osiguranim vratima, zgradama osiguranima od provale, dokumentiranim pravima pristupa (posjetitelji, zaposleni u drugim tvrtkama) ili utvrđenim područjima sigurnosti.

Kontrole pristupa obuhvaćaju mjere za osiguranje uređaja, mreže i aplikacija.

Kao mjere za osiguranje uređaja u vozilu primjenjuju se različite mjere: Mobilni krajnji uređaji čvrsto su ugrađeni u vozilo i imaju „secure boot", odnosno ne postoji mogućnost učitavanja stranog operacijskog sustava i pokretanja. Mobilni krajnji uređaji komuniciraju u šifriranom obliku s krajnjom točkom putem certifikata specifičnog za pojedini uređaj. Podaci se dalje u šifriranom obliku prenose unutar platforme RIO („Ubiquitous

encryption” ili „encryption everywhere”). Redovnim instaliranjem sigurnosnih ažuriranja krajnji se uređaji dovode u najnovije stanje sigurnosti (Patch-Management).

Kao mjere za osiguranje mreže primjenjuju se različite standardne mjere: Primjenjuju se prikladni (odgovarajuće tehničkom razvoju) uvjeti za lozinke (duljina, složenost, rok trajanja lozinke itd.). Ponovljeni neispravan unos kombinacije korisničkog imena / lozinke dovodi do (privremene) blokade korisničkog imena. Mreža poduzeća zaštićena je vatrozidom od nesigurnih otvorenih mreža. Uspostavljen je proces kojim se osigurava redovito instaliranje sigurnosnih ažuriranja na mobilne uređaje (OTA). Za razotkrivanje, odnosno izbjegavanje napada na mrežu poduzeća (Intranet) upotrebljavaju se odgovarajuće tehnologije (npr. sustavi za otkrivanje upada „intrusion detection”). Zaposlenicima se redovito podiže svijest o opasnostima i rizicima.

Kao mjere za osiguranje aplikacija primjenjuju se neke standardne mjere:

Relevantne aplikacije odgovarajućim su mehanizmima autentifikacije i autorizacije osigurane od neovlaštenog pristupa. Primjenjuju se prikladni (odgovarajuće tehničkom razvoju) uvjeti za lozinke (duljina, složenost, rok trajanja lozinke itd.). Za aplikacije s posebnom potrebom za zaštitu primjenjuju se strogi mehanizmi autentifikacije (npr. token, PKI). Ponovljeni neispravan unos kombinacije korisničkog imena / lozinke dovodi do (privremene) blokade korisničkog imena. Podaci koji se upotrebljavaju u relevantnom postupku nalaze se u šifriranom obliku na prijenosnom nosaču podataka. Uspješni pristupi i pokušaji pristupa aplikacijama protokoliraju se. Nastale datoteke protokola čuvaju se tijekom odgovarajućeg razdoblja (najmanje 90 dana) i provjeravaju se (nasumično).

Korisnička prava (pristupa i dohvata) osiguravaju se različitim mjerama, pri čemu su te mjere u načelu dodijeljene jednoj osobi kojoj je moguće utvrditi identitet. Dodjela prava u nadležnosti je operatera odgovornog za platformu i redovito se provjerava. Davanje prava na pristup slijedi tek nakon definiranog i dokumentiranog postupka. Izmjene u pravima na pristup provode se prema načelu četiri oka i dokumentiraju se u datoteci s popisom izmjena i oznakom verzije.

Kao mjere za kontrolu pristupa vozilu, odnosno upravljanja vozilom, primjenjuju se različite mjere: Prava na pristup definiraju i dokumentiraju se u okviru koncepta uloga / prava i prema zahtjevima određenog zadatka dodjeljuju se pojedinim ulogama. Uređene su posebne uloge / prava za tehničke administratore (koji, koliko je tehnički moguće, ne omogućuju pristup osobnim podacima). Uređene su posebne uloge / prava za tehničku podršku (koji ne sadržavaju tehnička administratorska prava).

Definiciju uloga / prava i dodjelu uloga / prava, koliko je tehnički i organizacijski moguće, ne izvršavaju iste osobe i taj je postupak (davanja dozvola) siguran od neovlaštenog pristupa te je vremenski ograničen. Izravna pristupanja bazi podataka zaobilaženjem koncepta uloga / prava moguća su samo za autorizirane administratore baze podataka. Upotreba privatnih nosača podataka uređena je pravilima, odnosno upotreba privatnih nosača podataka zabranjena je. Uspostavljena su obvezujuća pravila u pogledu pristupa podacima kod vanjskog održavanja, održavanja na daljinu i rada na daljinu. Uništavanje / odlaganje dokumenata i nosača

podataka prema propisima o zaštiti podataka (npr. rezač papira, sigurnosni spremnik) obavljaju pouzdana poduzeća ovlaštena za odlaganje otpada.

Koncept uloga / prava redovito se prilagođava izmjenama u strukturama organizacije rada (npr. nove uloge), a dodijeljene uloge / prava redovito preispituju npr. nadređene osobe i prema potrebi ih prilagođavaju ili povlače. Održava se redovita središnja kontrola u pogledu dodijeljenih standardnih profila. Pristupi kojima je došlo do izmjena (pisanje, brisanje) protokoliraju se, a nastale datoteke protokola čuvaju se tijekom odgovarajućeg razdoblja (najmanje 90 dana) i provjeravaju se (nasumično).

Kao opće mjere za osiguranje prosljeđivanja primjenjuju se različite standardne mjere:

Osobe kojima je povjeren zadatak daljnjeg prijenosa podataka unaprijed su upoznate sa sigurnosnim mjerama koje treba poduzeti. Skupina primatelja unaprijed se utvrđuje, tako da je moguća odgovarajuća kontrola (autentifikacija). Cijeli postupak daljnjeg prijenosa podataka utvrđen je i dokumentiran, a provedba konkretnog prijenosa podataka protokolira se, odnosno dokumentira (npr. potvrda prijma, račun). Osobe kojima je povjeren zadatak daljnjeg prijenosa podataka prethodno prolaze kroz provjeru vjerodostojnosti, potpunosti i ispravnosti.

Prije provedbe konkretnog prijenosa podataka provjerava se adresa primatelja (npr. adresa e-pošte). Prijenos podataka putem interneta odvija se u šifriranom obliku (npr. šifriranje datoteke). Integritet prenesenih podataka jamči se, koliko je tehnički moguće, primjenom potpisivanja (digitalni potpis). Elektroničke potvrde o prijmu arhiviraju se u odgovarajućem obliku. Neželjeni prijenosi podataka putem interneta sprečavaju se odgovarajućim tehnološkim rješenjima (npr. proxy, vatrozid).

Nadalje, kao mjere za provedbu pravila o razdvajanju primjenjuju se sljedeće standardne mjere:

Uspostavljena su obvezujuća pravila u pogledu ograničenja svrhe obrade radi pridržavanja pravila o razdvajanju. Podaci prikupljeni za određenu svrhu pohranjuju se odvojeno od podataka prikupljenih u druge svrhe. IT sustavi u primjeni dopuštaju odvojeno pohranjivanje podataka (putem svojstva više klijenata ili koncepata pristupa). Razdvajanje podataka odvija se u testnim i proizvodnim sustavima. Kod pseudonimiziranih podataka šifrarnik koji omogućuje ponovnu identifikaciju sprema se, odnosno pohranjuje odvojeno. Pri ugovorenom provođenju obrade ili prijenosu funkcije Izvođač odvojeno obrađuje podatke različitih naručitelja. Postojeći koncepti uloga / prava omogućuju svojim ustrojem logičko razdvajanje obrađenih podataka.

4. Jamstvo cjelovitosti

Kao mjere za provedbu protokoliranja unosa podataka primjenjuju se različite standardne mjere:

Protokoliraju se izmjene prava pristupa kao i cjelokupne administrativne aktivnosti. Protokoliraju se pristupi s pisanjem (unosi, izmjene, brisanja) i promjene na podatkovnim poljima (npr. sadržaj novog unesenog ili izmijenjenog skupa podataka). Protokoliraju se prijenosi (npr. preuzimanje) i prijave korisnika.

Korišteni dokumenti za prikupljanje podataka evidentiraju se i arhiviraju radi sljedivosti. Protokoliranje se provodi navođenjem datuma, vremena, korisnika, vrste aktivnosti, aplikacije i rednog broja skupa podataka. Dokumentiraju se postavke protokoliranja.

Za datoteke protokola moguć je pristup samo za čitanje. Skupina korisnika s pravom pristupa datotekama protokola vrlo je ograničena (npr. na administratora, službenika za zaštitu podataka, revizora). Datoteke protokola čuvaju se tijekom odgovarajućeg razdoblja (npr. 1 godinu), a zatim se brišu u skladu s propisima o zaštiti podataka. Datoteke protokola redovno se automatski ocjenjuju. Datoteke protokola ocjenjuju se koliko je to moguće u pseudonimiziranom obliku.

5. Jamstvo raspoloživosti

Arhitektura je osigurana od gubitka podataka internim mehanizmima repliciranja unutar platforme AWS-a. Nadalje, kao mjere za osiguranje objekta primjenjuju se sljedeće standardne mjere AWS-a:

Primjenjuju se mjere protupožarne zaštite (npr. protupožarna vrata, dojavljivači dima, protupožarni zidovi, zabrana pušenja). Računalna oprema zaštićena je od poplave (npr. prostorija s računalima na 1. katu, dojavljivač vode). Primjenjuju se mjere protiv podrhtavanja (npr. prostorija s računalima nije u blizini brze ceste, željezničke pruge, prostorija sa strojevima). Računalna oprema osigurana je od elektromagnetskih polja (npr. čelične ploče u vanjskim zidovima). Primjenjuju se mjere protiv vandalizma i krađe (npr. kontrola pristupa). Računalna oprema nalazi se u klimatiziranim prostorijama (temperaturu i vlagu u zraku regulira klimatizacijski sustav). Računalna oprema prenaponskom je zaštitom osigurana od vršnih prenapona. Primjenjuju se mjere za osiguranje neometanog i neprekidnog napajanja strujom (npr. UPS uređaji, agregati za slučaj nužde).

Baze podataka redovito se osiguravaju u obliku sigurnosnih rezervnih kopija unutar platforme AWS-a. Koncept stvaranja sigurnosnih kopija dokumentira se i redovito provjerava i ažurira. Mediji za sigurnosno kopiranje zaštićeni su od neovlaštenog pristupa. Korišteni programi za sigurnosno kopiranje odgovaraju najnovijim standardima kvalitete i prema tome se redovito ažuriraju. Uspostavljen je redundantan podatkovni centar (udaljen od mjesta obrade podataka) koji može nastaviti s obradom podataka u slučaju katastrofe. Različite mjere za kontrolu raspoloživosti dokumentirane su u planu AWS-a za upravljanje izvanrednim situacijama.

Prije nego što se dodijeli ugovor za obradu podataka, Izvođač se provjerava pažljivo i prema utvrđenim kriterijima (tehničke i organizacijske mjere). Pritom se od Izvođača traži da detaljno izloži tehničke / organizacijske mjere za zaštitu podataka koje primjenjuje (odgovaranje na katalog pitanja ili koncept zaštite podataka) i koje se provjeravaju. Ovisno o količini i osjetljivosti obrađenih podataka, ova provjera obavlja se prema potrebi i na lokaciji Izvođača. Pri odabiru izvođačâ uzimaju se u obzir odgovarajući certifikati (npr. ISO 27001). Utvrđivanje prikladnosti izvođača dokumentira se u odgovarajućem i sljedivom obliku.

Za osnovu ugovornog odnosa Naručitelj i Izvođač sklapaju ugovor o provođenju obrade. U tom ugovoru detaljno u pisanom obliku utvrđene su ovlasti i odgovornosti, te obveze obiju ugovornih strana. Ako se sjedište ugovornog pružatelja usluga nalazi izvan EU-a, odnosno EGP-a, primjenjuju se standardne ugovorne klauzule

EU-a. Ugovorom je utvrđeno da Izvođač smije obrađivati podatke samo u okviru uputa koje je dobio od Naručitelja. Izvođač je obvezan bez odgode obavijestiti Naručitelja ako smatra da je određena uputa u suprotnosti s propisima iz područja zaštite podataka. Da bi se zaštitila prava zainteresiranih, u ugovoru o provođenju obrade određuje se da Izvođač mora pružiti odgovarajuću podršku Naručitelju, ako je to potrebno npr. u slučaju davanja informacija zainteresiranim stranama.

U daljnjem tijeku ugovorenog provođenja obrade Naručitelj kontrolira rezultate rada Izvođača u pogledu forme i sadržaja. Redovito se provjerava pridržava li se Izvođač predmetnih tehničkih i organizacijskih mjera. Za to se prvenstveno dostavljaju aktualne ovjere ili odgovarajući certifikati, odnosno dokazuje se da su IT sigurnost ili zaštita podataka provjereni. Ako su angažirani podizvođači, ugovorom je utvrđeno da se kontroliraju na odgovarajući način.

6. Jamstvo otpornosti sustava

Infrastruktura u oblaku AWS-a izgrađena je kao jedno od najfleksibilnijih i najsigurnijih okruženja računalstva u oblaku. Oblikovana je tako da pruža optimalnu raspoloživost pri potpunoj odvojenosti klijenata i nudi izrazito nadogradivu pouzdanu platformu koja omogućuje klijentima da prema potrebi brzo i sigurno prošire aplikacije i sadržaje diljem svijeta. Usluge AWS-a neovisne su o sadržaju jer nude svim klijentima jednako visoku razinu sigurnosti, neovisno o vrsti sadržaja ili geografskoj regiji u kojoj su sadržaji pohranjeni.

Računalni centri AWS-a s visokom razinom sigurnosti na svjetskoj razini primjenjuju elektroničke mjere nadzora najnovijeg stupnja tehničkog razvoja i višerazinske sustave kontrole pristupa. U računalnim centrima u svako doba nalazi se obučeno zaštitarsko osoblje, a pristup se daje prema načelu najmanjih prava i isključivo u svrhe administracije sustava.

7. Postupak za ponovnu uspostavu raspoloživosti osobnih podataka nakon fizičkog ili tehničkog incidenta

Računalni centri AWS-a uspostavljeni su u klasterima u različitim regijama u svijetu. Svi računalni centri spojeni su na mrežu i opslužuju klijente; nijedan računalni centar nije isključen. U slučaju ispada podatkovni promet klijenata automatskim se putem premješta dalje od pogođenih područja. Središnje aplikacije isporučuju se u konfiguraciji N+1, tako da u slučaju ispada računalnog centra postoji dostatan kapacitet za raspodjelu podatkovnog prometa na preostale lokacije.

AWS nudi fleksibilnost za smještanje jedinica i pohranjivanje podataka unutar više geografskih regija kao i u više zona dostupnosti („availability zones") unutar pojedinačnih regija. Svaka zona dostupnosti razvijena je kao neovisna zona za slučaj ispada. To znači da su unutar tipičnog gradskog područja zone dostupnosti fizički odijeljene i nalaze se u područjima s nižim rizikom od poplave (ovisno o regiji, postoje različite kategorizacije poplavnih zona). Osim osiguranog samostalnog i neprekidnog napajanja strujom i generatora za slučaj nužde na samoj lokaciji, sve zone dostupnosti napajaju se strujom preko različitih električnih mreža od neovisnih

elektrodistributera kako bi se pojedinačna mjesta ispada smanjila na najmanju moguću mjeru. Sve zone dostupnosti redundantno su povezane putem više pružatelja Tier 1 mreža za prijenos.

Tim tvrtke Amazon provodi uobičajene dijagnostičke postupke za rješavanje incidenata kako bi se uklonili incidenti kritični za rad poduzeća. Stručno osoblje nudi neprekidnu spremnost u bilo koje doba dana, sedam dana u tjednu i 365 dana u godini kako bi se štetni događaji prepoznali te uklonili zajedno s njihovim učincima.

8. Postupak redovne provjere, ocjenjivanja i evaluacije učinkovitosti tehničkih i organizacijskih mjera

Smjernice i upute dostupne u poduzećima, odnosno standardi koji se primjenjuju za sigurnost informacija, primjenjuju se i u pogledu uvođenja i rada platforme RIO. U poduzeću su uspostavljene funkcije za zaštitu podataka i sigurnost informacija (službenik za zaštitu podataka i „information security officer"). Zaposlenici su obvezani na čuvanje tajnosti podataka i informirani o mjerama za sigurnost podataka, odnosno IT sigurnost putem brošura, letaka, uputa na intranetu itd.

Provjeravaju se interni postupci u pogledu pridržavanja tehničkih i organizacijskih mjera za sigurnost podataka putem revizije, provjere sigurnosti informacija i zaštite podataka.

Aktivnosti obrade i mjere za sigurnost podataka dokumentiraju se u popisu aktivnosti obrade. Učinkovitost mjera redovito se provjerava (interno i putem vanjskih provjera).