Pogodba o obdelavi podatkov (v skladu s členom 28 SUVP)

ki jo skleneta

uporabnik (kot je opredeljen v glavni pogodbi)

(v nadaljevanju »**naročnik**«)

in

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

(v nadaljevanju »**izvajalec**«)
(naročnik in izvajalec v nadaljevanju posamezno **»stranka«** in skupaj **»stranki«**).

Preambula

(A) Ta pogodba o obdelavi podatkov (v nadaljevanju »**pogodba**«) se uporablja za vse dejavnosti, pri katerih izvajalec pride v stik z osebnimi podatki (kot so opredeljeni v točki 1.5) naročnika, tretjih strank ali drugih zadevnih oseb v zvezi z dejavnostjo, opisano v točki 2, iz splošnih okvirnih pogojev o uporabi platforme in v okviru teh pogojev sklenjenih posameznih pogodb za dodatne storitve (v nadaljevanju »**glavna pogodba**«).

(B) V okviru te pogodbe deluje naročnik kot odgovorna oseba in izvajalec kot obdelovalec podatkov pri obdelavi podatkov v skladu s členom 28 SUVP (kot je opredeljeno spodaj).

Stranki se dogovorita naslednje:

1 Opredelitve in razlaga

1.1 »**Evropska zakonodaja**« pomeni zakonodajo, ki se uporablja v Evropski uniji, zakone, ki se uporabljajo v trenutnih državah članicah Evropske unije, in zakone, ki se uporabljajo v posameznih državah, ki naknadno postanejo članice Evropske unije.

1.2 »**Evropska zakonodaja o varstvu podatkov**« pomeni zakonodajo o obdelavi osebnih podatkov, ki se uporablja v Evropski uniji (predvsem SUVP), zakone o obdelavi osebnih podatkov, ki se uporabljajo v trenutnih državah članicah Evropske unije (predvsem najnovejša različica BDSG), in zakone o obdelavi osebnih podatkov, ki se uporabljajo v posameznih državah, ki naknadno postanejo članice Evropske unije.

1.3 »**SUVP**« pomeni »Uredbo (EU) 2016/679 Evropskega Parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)«.

1.4 »**BDSG**« pomeni nemški zvezni zakon o varstvu osebnih podatkov (Bundesdatenschutzgesetz).

1.5 »**Osebni podatki**« imajo pomen, opredeljen v BDSG/SUVP.

2 Predmet obdelave podatkov/obveznosti naročnika

2.1 Ta pogodba ureja obveznosti strank v povezavi z obdelavo osebnih podatkov naročnika, ki jo izvede izvajalec, v okviru glavne pogodbe iz Priloge 1.

2.2 Predmet in trajanje obdelave, način in namen obdelave, vrsta osebnih podatkov, kategorije zadevnih oseb ter obveznosti in pravice upravljavca podatkov so opredeljeni v Prilogi 1 k tej pogodbi in specifikacijah glavne pogodbe.

2.3 Naročnik je še vedno odgovorna oseba v smislu SUVP in jamči za zakonitost obdelave osebnih podatkov zadevnih oseb (voznika in po potrebi drugih oseb). V povezavi s tem naročnik izpolnjuje zlasti svojo obsežno obveznost obveščanja in za obdelavo osebnih podatkov zagotavlja ustrezno pravno podlago z vidika varstva podatkov (npr. sklenitev podjetniškega sporazuma, omejitev obdelave na namene zaposlitvenega razmerja).

3 Obveznosti izvajalca

3.1 Izvajalec obdeluje osebne podatke naročnika izključno za namene, opredeljene v Prilogi 1, in v okviru glavne pogodbe ter v skladu z navodili naročnika, navedenimi v pogodbi in Prilogi 1; izvajalec osebnih podatkov v skladu s to pogodbo ne sme obdelovati za noben drug namen. To ne velja za obdelavo za lastne namene v skladu s točko 8.3.4 glavne pogodbe, ki ni del te pogodbe. Izdelava kopij ali dvojnikov osebnih podatkov brez vednosti naročnika ni dovoljena. Izjema so varnostne kopije, ki so nujne za zagotavljanje pravilne obdelave podatkov, in podatki, ki so potrebni za izpolnjevanje zakonskih obveznosti glede hrambe.

3.2 Po končanem zagotavljanju storitev v zvezi z obdelavo mora izvajalec vse osebne podatke naročnika izročiti naročniku in/ali jih izbrisati v skladu z zahtevami o varstvu podatkov, če jih ne omejujejo zakonski predpisi glede obdobja hranjenja in če jih izvajalec ne obdeluje za lastne namene v skladu s točko 8.3.4 glavne pogodbe, ki niso vključeni v to pogodbo. Enako velja za testni in odpadni material. Popoln izbris oz. izročitev podatkov naročniku se naročniku na zahtevo potrdi pisno z navedbo datuma.

3.3 Če je to vključeno v obseg storitev, izvajalec naročnika podpira pri izpolnjevanju pravic zadevnih oseb (obveščanje, popravki, ugovor, izbris) po ustreznih navodilih naročnika.

3.4 Izvajalec potrdi, da je – če zakon tako zahteva – imenoval notranjega nadzornika za varstvo podatkov (gl. poglavje 38 BDSG, člen 37 SUVP).

3.5 Izvajalec se zaveže, da bo naročnika nemudoma obvestil o rezultatu preverjanj organov za nadzor varstva podatkov, povezanih z obdelavo podatkov naročnika. Vse ugotovljene pomanjkljivosti izvajalec v razumnem roku odpravi in to sporoči naročniku.

3.6 Obdelava podatkov, ki jo izvedejo izvajalec in s strani naročnika odobreni podizvajalci, se izvaja izključno na ozemlju Zvezne republike Nemčije, v državi članici Evropske unije ali v drugi pogodbeni državi, ki ima sklenjen sporazum o Evropskem gospodarskem prostoru. Za vsakršen premik v katero drugo državo (v nadaljevanju »**tretja država**«) je potrebno predhodno izrecno soglasje naročnika in se poleg tega lahko izvede le, če so izpolnjeni posebni pogoji za izvoz podatkov v tretje države (gl. člen 40 in naslednji SUVP). Poleg tega je treba zagotoviti informacije iz Priloge 1 in po potrebi priložiti dodatno (pogodbeno) dokumentacijo.

3.7 Izvajalec mora zaposlene, ki sodelujejo pri izvajanju del, seznaniti z zadevnimi določbami o varstvu podatkov in zahtevati, da ohranjajo tajnost podatkov (gl. odstavek 3b člena 28 SUVP), ter z ustreznimi koraki zagotavljati, da vsi zaposleni osebne podatke obdelujejo samo po navodilih naročnika.

3.8 Izvajalec v času veljavnosti pogodbe redno preverja upoštevanje predpisov o varstvu podatkov iz te pogodbe in dokumentiranih navodil naročnika. Rezultati preverjanj, ki so pomembni za obdelavo podatkov naročnika, se na zahtevo predložijo naročniku. Ukrepi za nadzor so opisani v konceptu varstva podatkov, ki se na zahtevo predloži naročniku.

3.9 Izvajalec mora ob upoštevanju narave obdelave pomagati naročniku z ustreznimi tehničnimi in organizacijskimi ukrepi, kolikor je to mogoče, pri izpolnjevanju njegovih obveznosti, da odgovori na zahteve za uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki, iz poglavja III SUVP. Stroške, ki pri tem nastanejo izvajalcu, plača naročnik.

3.10 Izvajalec mora ob upoštevanju narave obdelave in informacij, ki so mu dostopne, pomagati naročniku pri izpolnjevanju obveznosti iz členov 32 do 36 SUVP.

4 Tehnični in organizacijski ukrepi za zagotovitev varnosti podatkov

4.1 Izvajalec sprejme ustrezne tehnične in organizacijske ukrepe za varstvo podatkov (gl. člen 32 SUVP). Izvajalec je zlasti zavezan k izvajanju tehničnih in organizacijskih ukrepov, pogodbeno dogovorjenih v Prilogi 2 k tej pogodbi. Te ukrepe mora izvajalec v času pogodbenega razmerja prilagajati razvoju na tehničnem in organizacijskem področju, ne da bi pri tem zmanjšal raven zaščite. O bistvenih spremembah se je treba dogovoriti pisno.

4.2 Izvajalec naročniku na zahtevo predloži dokaze o dejanskem izpolnjevanju tehničnih in organizacijskih ukrepov.

4.3 Izvajalec mora voditi ustrezno dokumentacijo o obdelavi podatkov, ki jo lahko naročnik uporabi kot dokaz o pravilni obdelavi podatkov. Dokaz se lahko predloži tudi z odobrenim postopkom certificiranja v skladu s členom 42 SUVP.

5 Podizvajalci

5.1 Izvajalcu se odobri vključitev podizvajalcev, navedenih v Prilogi 1.

5.2 Vključitev dodatnih podizvajalcev se na splošno odobri. Vendar mora izvajalec naročnika obvestiti o vsaki nameravani spremembi glede zaposlitve dodatnih podizvajalcev ali njihove zamenjave; naročnik lahko nameravanim spremembam nasprotuje. Kot podpogodbena razmerja v smislu te uredbe se ne štejejo storitve, ki jih za izvajalca izvedejo tretje osebe kot pomožno storitev v pomoč pri izvajanju naročila. Sem spadajo na primer telekomunikacijske storitve, čiščenje, revidiranje in odstranjevanje nosilcev podatkov. Vendar mora izvajalec za zagotavljanje zaščite in varnosti podatkov naročnika tudi pri pomožnih storitvah, za katere pooblasti tretje osebe, skleniti ustrezne in zakonite pogodbene dogovore ter izvajati nadzorne ukrepe.

5.3 Kadar izvajalec zaposli podizvajalca, mora zagotoviti, da za podizvajalca na podlagi (i) pogodbe, ki jo skleneta podizvajalec in izvajalec, ali (ii) drugega pravnega akta v skladu z evropsko zakonodajo o varstvu podatkov veljajo enake obveznosti varstva podatkov, kot veljajo za izvajalca v skladu s to pogodbo. Pri tem mora izvajalec poskrbeti zlasti za to, da podizvajalec zagotovi zadostna jamstva za izvajanje ustreznih tehničnih in organizacijskih ukrepov na tak način, da obdelava osebnih podatkov izpolnjuje zahteve SUVP. Izvajalec naročniku na pisno zahtevo predloži informacije o bistvenih vsebinskih delih pogodbe in izvajanju obveznosti glede varstva podatkov v podpogodbenem razmerju, po potrebi z odobritvijo vpogleda v ustrezno pogodbeno dokumentacijo. Poslovne pogoje lahko izvajalec pri tem počrni. Naročnik je dolžan varovati zaupnost pridobljenih informacij.

6 Pravice nadzora

6.1 Naročnik ima pravico, da bodisi sam bodisi prek ustrezne pooblaščene tretje osebe preverja izpolnjevanje obveznosti iz te pogodbe (vključno s podanimi navodili).

6.2 Izvajalec naročniku zagotavlja ustrezno podporo pri preverjanjih. Predvsem mu omogoči dostop do opreme za obdelavo podatkov in zagotovi potrebne informacije.

6.3 Če se pri preverjanju ugotovi, da izvajalec in/ali obdelava ne izpolnjujeta zahtev te pogodbe in/ali evropske zakonodaje o varstvu podatkov, izvajalec sprejme vse korektivne ukrepe, potrebne za zagotovitev izpolnjevanja zahtev te pogodbe in/ali evropske zakonodaje o varstvu podatkov.

6.4 Stroške, ki pri preverjanju nastanejo naročniku, plača naročnik sam. Za stroške, ki pri preverjanju s strani naročnika nastanejo izvajalcu, lahko izvajalec zahteva, da jih plača naročnik, če ta izvede, bodisi sam bodisi prek koga drugega, več preverjanj v koledarskem letu.

6.5 O preverjanjih mora biti izvajalec pravočasno obveščen in ne smejo nesorazmerno ovirati njegovega poslovanja.

7 Obveznosti obveščanja

Če izvajalec meni, da katero od naročnikovih navodil krši evropsko zakonodajo o varstvu podatkov, o tem nemudoma obvesti naročnika. Če naročnik spornega navodila ne spremeni ali izrecno potrdi, navodila ni treba upoštevati. Materialnopravno preverjanje navodil ni dolžnost izvajalca.

Če izvajalec pri obdelavi podatkov ugotovi napake ali nepravilnosti ali sumi kršitev varstva podatkov (v nadaljevanju skupno »**incident**«), o tem takoj ustrezno obvesti naročnika. Naročnik mora incident, vključno z vsemi dejstvi in okoliščinami, posledicami incidenta ter vsemi korekcijskimi ukrepi, dokumentirati in te dokumentirane informacije na zahtevo nemudoma v pisni ali elektronski obliki posredovati naročniku.

8 Odgovornost in odškodnina

8.1 Izvajalec odgovarja za škodo, ki nastane zaradi napake in/ali hude malomarnosti izvajalca ali njegovih zastopnikov. Za škodo, ki je posledica lahke malomarnosti izvajalca ali njegovih zastopnikov, izvajalec odgovarja le, če gre za kršitev temeljne obveznosti. Temeljne obveznosti so bistvene pogodbene obveznosti, ki omogočajo pravilno izvedljivost pogodbe ter za katere je naročnik zaupal in se upravičeno zanašal na to, da se izvajajo. Pri lahki malomarnosti v zvezi s kršenjem takšnih temeljnih obveznosti je odgovornost izvajalca omejena na škodo, ki jo je običajno mogoče predvideti.

8.2 Naročnik plača odškodnino izvajalcu za vse zahtevke tretjih oseb (vključno z osebami, na katere se podatki nanašajo, in/ali organi za varstvo podatkov), škodo in stroške, ki so posledica naročnikovega kršenja določil te pogodbe in/ali evropske zakonodaje o varstvu podatkov; to ne velja, če naročnik ni zagrešil kršitve ali če je izvajalec prispeval h kršitvi.

9 Trajanje pogodbe

Trajanje te pogodbe je enako trajanju glavne pogodbe. Ko se iz katerega koli razloga prekine glavna pogodba, se samodejno prekine tudi ta pogodba. To ne vpliva na prekinitev pogodbe zaradi pomembnega razloga.

10 Ostalo

10.1 Storitve izvajalca iz te pogodbe se plačajo v skladu s pravilnikom o nadomestilu stroškov, opredeljenim v glavni pogodbi.

10.2 Če so osebni podatki naročnika pri izvajalcu ogroženi zaradi ukrepov tretjih oseb (na primer zaplembe ali zasega), zaradi stečajnega postopka ali postopka poravnave ali zaradi drugih podobnih dogodkov, izvajalec to nemudoma sporoči naročniku.

10.3 Če so posamezna določila te pogodbe neveljavna ali postanejo neveljavna, to ne vpliva na veljavnost preostalih določil. Stranki se v primeru neveljavnosti katere od klavzul dogovorita o nadomestni ureditvi, ki je z vsebinskega in gospodarskega vidika usklajena z namenom pogodbe.

10.4 V primeru izstopa Velike Britanije iz Evropske unije se izvajalec že zdaj zavezuje, da bo sklenil vse dogovore in izvedel vse ukrepe, potrebne za to, da bo obdelava podatkov, ki je predmet te pogodbe, v Veliki Britaniji po izstopu potekala v skladu s pravili o varstvu podatkov. Če v času izstopa Evropska komisija še ne bo sprejela nikakršne pozitivne odločbe o ustreznosti, so to z današnjega vidika zlasti standardna določila o varstvu podatkov v skladu z odstavkom 2c člena 46 za posredovanje osebnih podatkov obdelovalcem s sedežem v tretjih državah, v katerih ni zagotovljena ustrezna raven zaščite.

Če izvajalec teh obveznosti ne izpolni, ima naročnik po izstopu Velike Britanije iz Evropske unije od izvajalca pravico zahtevati, da zadevne storitve izvede povezano podjetje oz. del podjetja s stalnim sedežem na ozemlju Evropske unije, ne da bi pri tem za naročnika nastale dodatne obremenitve ali dodatni stroški.

10.5 Ta pogodba o obdelavi podatkov obstaja v 18 jezikovnih različicah, pri čemer ima v primeru odstopanj prednost originalna različica v nemškem jeziku.

10.6 Osnova tej pogodbi je pravo Zvezne republike Nemčije brez konvencije Združenih narodov o pogodbah o mednarodni prodaji blaga. Izključno pristojno sodišče je sodišče v Münchnu.

10.7 Spodnji prilogi sta sestavni del pogodbe:

Priloga 1 – Opis obdelave podatkov
Priloga 2 – Tehnični in organizacijski ukrepi

PRILOGA 1 – Opis obdelave podatkov

1 Glavna pogodba

Glavna pogodba v smislu točke 2.1 glavnega dela pogodbe so »Splošni okvirni pogoji o uporabi platforme«.

Naziv/stranka: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19–21, 80807 München/**uporabnik**

2 Predmet in trajanje naročila

Predmet naročila je naveden v točki 1 (*Predmet*) in točki 8 (*Podatki uporabnika in varstvo podatkov*) glavne pogodbe; trajanje naročila je navedeno v točki 7 (*Sklenitev pogodbe, trajanje pogodbe in pravice do prekinitve*) glavne pogodbe.

3 Obseg, način in namen obdelave podatkov/postopki obdelave podatkov

Obseg, način in namen obdelave osebnih podatkov so navedeni v točki 8 glavne pogodbe.

Podrobnejši opis predmeta naročila glede obsega, načina in namena:

da lahko izvajalec izvede ponujene storitve (opredeljene v glavni pogodbi), mora prek sistema Connected Vehicle ali Mobile Device zbrati osebne podatke naročnika (in morebitne osebne podatke, ki jih je prenesla tretja stranka, s katero se je uporabnik dogovoril za izvedbo storitev), ki jih potrebuje za izvedbo storitev, ter jih prenesti na svojo platformo in jih tam shraniti. Podatke, shranjene na platformi, izvajalec obdela v obsegu, potrebnem za izvedbo storitev (na primer za to, da na podlagi osebnih podatkov analizira in ovrednoti način voznikove vožnje ter uporabo sistema Connected Vehicle ali Mobile Device in na podlagi ugotovitev predloži naročniku ponudbe, posebej prilagojene njegovim potrebam, na primer vozniška usposabljanja, podrobnosti o opremi ter predloge za povečanje učinkovitosti). Obseg, način in namen so natančneje razvidni zlasti iz posameznih pogodb, ki se sklenejo naknadno.

4 Osebe, na katere se nanašajo osebni podatki (kategorije takšnih oseb)

Obdelava podatkov zadeva naslednje osebe:

- **voznike in druge zaposlene** (zaposlene v lastni družbi naročnika), npr. delavce, pripravnike, kandidate, nekdanje zaposlene;
- **voznike**, ki niso zaposleni;
- **kontaktne osebe** nakladalcev/razkladalcev ali drugih poslovnih partnerjev naročnika in
- **zaposlene v koncernu** (zaposlene v drugih družbah skupine naročnika).

5 Vrsta osebnih podatkov

V obdelavo podatkov so vključene naslednje vrste osebnih podatkov:

- ime voznika in identifikacijska številka voznika;
- identifikacijska številka vozila;
- podatki o lokaciji;
- podatki o času vožnje in počitka;
- podatki o načinu vožnje;
- podatki o stanju sistema Connected Vehicle;
- podatki o stanju priklopnika;
- podatki o stanju nadgradenj oz. konstrukcij, agregatov in drugih sestavnih delov vozila;
- podatki o stanju naprav IS, če so priključene;
- podatki o stanju sistema Mobile Device;
- podatki o tovoru;
- pogodbeni podatki in
- kontaktni podatki kontaktnih oseb nakladalcev/razkladalcev ali drugih poslovnih partnerjev naročnika.

6 Dokumentirana navodila

Naročnik z dokumentiranimi navodili izvajalcu naroča, naj osebne podatke obdela v skladu s točko 8 glavne pogodbe. To vključuje predvsem naslednjo obdelavo:

- Osebni podatki se prek sistema Connected Vehicle ali Mobile Device prenesejo na platformo v oblaku in se tam shranijo.
- Osebni podatki se v skladu s to pogodbo obdelajo le, če je to potrebno za izpolnjevanje določil glavne pogodbe; to ne vpliva na točko 8.3.4 glavne pogodbe.
- Izvajalec posreduje osebne podatke tretji stranki (kot je opredeljena v glavni pogodbi), če in kolikor jih ta potrebuje, da izvede svoje storitve (kot so opredeljene v glavni pogodbi) za naročnika.
- Izvajalec na podlagi osebnih podatkov analizira in ovrednoti način voznikove vožnje ter uporabo sistema Connected Vehicle in na podlagi ugotovitev predloži naročniku ponudbe, posebej prilagojene njegovim potrebam, na primer vozniška usposabljanja, podrobnosti o opremi ter predloge za povečanje učinkovitosti.

7 Kraj obdelave podatkov

- Nemčija.
- Združeno kraljestvo; če se podatki za namene IT-gostovanja in/ali IT-podpore obdelujejo na ozemlju Evropske unije, se sklenejo ustrezne pogodbe o obdelavi podatkov.
- Če izvajalec za namene IT-gostovanja in/ali IT-podpore najame podizvajalca zunaj Evropske unije (več podrobnosti v točki 8 te Priloge 1), se posredovanje osebnih podatkov izvede na podlagi standardnih

pogodbenih klavzul/standardnih določil o varstvu podatkov, sklenjenih med izvajalcem in podizvajalcem, za posredovanje osebnih podatkov obdelovalcem v tretjih državah v skladu z odstavkom 2c člena 46 SUVP.

8 Podizvajalci

Izvajalec najame naslednje podizvajalce (ki lahko po potrebi najamejo druge podizvajalce):

Št.	Podizvajalec (podjetje, naslov, kontaktna oseba)	Obdelane kategorije podatkov	Postopki obdelave/namen podpogodbene obdelave podatkov
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Vsi osebni podatki na platformi, ki so povezani s prodajnim delom (tj. kjer se stranka na platformi registrira in lahko opravlja naročila).	Gostovanje na platformi
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Vsi osebni podatki na platformi, ki so povezani s prodajnim delom (tj. kjer se stranka na platformi registrira in lahko opravlja naročila).	IT-podpora v zvezi s platformo
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 ZDA https://aws.amazon.com/de/compliance/contact/	Vsi drugi osebni uporabniški podatki, ki se prek vozila posredujejo izvajalcu.	Gostovanje na platformi/IT-podpora v zvezi s platformo
4	V prihodnje morda namesto št. 3: Amazon Webservices (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 ZDA https://aws.amazon.com/de/compliance/contact/	Vsi drugi osebni uporabniški podatki, ki se prek vozila posredujejo izvajalcu.	Gostovanje na platformi
5	MAN Service und Support GmbH Dachauer Straße 667	Vsi osebni podatki, ki so potrebni za obravnavo povpraševanj strank v	Podpora 1. stopnje

	80995 München Nemčija	okviru podpore 1. in 2. stopnje.	
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 ZDA	Vsi osebni podatki, ki so potrebni za obravnavo izstavljanja računov/obdelavo naročil.	Gostovanje na platformi (EU Tenant – Gehosted by Amazon Web Services (EU) – glej št. 4
7	MAN Truck & Bus AG Dachauer Str. 667 80995 München Nemčija	Vsi drugi osebni uporabniški podatki, ki se posredujejo izvajalcu prek sistemov Connected Vehicle in/ali Mobile Device.	Gostovanje na platformi
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Nemčija	Vsi drugi osebni uporabniški podatki, ki se posredujejo izvajalcu prek vozil TBM1/2.	Gostovanje na platformi
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Švedska	Vsi drugi osebni uporabniški podatki, ki se prek vozila posredujejo izvajalcu.	Gostovanje na platformi
10	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hannover Nemčija	Vsi drugi osebni uporabniški podatki, ki se prek vozila posredujejo izvajalcu.	Gostovanje na platformi

PRILOGA 2 – Tehnični in organizacijski ukrepi
Tehnični in organizacijski ukrepi, ki jih mora sprejeti izvajalec za zagotovitev ravni zaščite, ki ustreza stopnji tveganja, so opisani v konceptu varstva podatkov za platformo RIO in vključujejo zlasti naslednje:

1. Psevdonimizacija

Če se osebni podatki uporabijo za namene ovrednotenja, ki so izvedljivi tudi s psevdonimiziranimi podatki, se uporabijo tehnike psevdonimizacije. V tem primeru se najprej za vsako podatkovno polje vnaprej določi, ali mora biti psevdonimizirano, ker bi sicer omogočalo razpoznavnost zadevne osebe. Kode psevdonimizacije se shranijo v podatkovni sef, ki se zaščiti s čim večjo omejitvijo dostopa.

2. Šifriranje

Mobilna terminalska oprema komunicira s končno točko v šifrirani obliki na podlagi individualnega certifikata opreme. Podatki se na platformi RIO posredujejo naprej v šifrirani obliki (»Ubiquitous encryption« ali »encryption everywhere«).

3. Zagotavljanje zaupnosti

Za vse zaposlene velja obveznost nerazkrivanja in vsi se pisno zavežejo, da bodo ohranjali tajnost podatkov.

Uporabljena IT-infrastruktura se prek Amazon Web Services da na voljo v okviru oblaka (IaaS & PaaS). Nadzor dostopa omogoči upravljavec podatkovnega centra Amazon Web Services: visoko zaščiteni računalniški centri Amazon Web Services uporabljajo najsodobnejše ukrepe elektronskega nadzora in sisteme večstopenjskega nadzorovanja dostopa. V računalniških centrih je nenehno prisotno usposobljeno varnostno osebje in dostop je strogo zavarovan z načelom najmanjših pravic ter omogočen izključno skrbnikom sistemov.

Dostop do komponent strojne opreme (odjemalci) podjetja TB Digital Services GmbH poteka v skladu z veljavnimi standardnimi ukrepi, ki ustrezajo v posameznem primeru. Ti med drugim vključujejo omejitve dostopa z izolirnimi napravami (vozlišča), opremo za videonadzor, alarmni sistem in/ali varnostno službo, elektronsko ali mehansko varovana vrata, protivlomno zaščitene objekte, dokumentiranje dovoljenih dostopov (obiskovalci, zunanji sodelavci) in določena varnostna območja.

Nadzor dostopa obsega ukrepe za zaščito opreme, omrežja in aplikacij.

Za zaščito opreme v vozilu se uporabljajo različni ukrepi: mobilna terminalska oprema je vgrajena v vozilo in omogoča Secure Boot, kar pomeni, da ni mogoče naložiti in zagnati nobenega zunanjega operacijskega sistema. Mobilna terminalska oprema komunicira s končno točko v šifrirani obliki na podlagi individualnega certifikata opreme. Podatki se na platformi RIO posredujejo naprej v šifrirani obliki (»Ubiquitous encryption« ali »encryption everywhere«). Mobilna terminalska oprema z rednim nalaganjem varnostnih posodobitev zagotavlja najbolj izpopolnjeno stopnjo zaščite (Patch-Management).

Tudi za zaščito omrežja se uporabljajo različni ukrepi: za gesla veljajo ustrezne specifikacije (skladne z najsodobnejšo tehniko) (dolžina, kompleksnost, trajanje veljavnosti gesla itd.). Večkraten napačen vnos kombinacije uporabniškega imena/gesla povzroči (začasno) blokado uporabniškega imena. Omrežje podjetja je s požarnim zidom zaščiteno pred nezaščitenimi javnimi omrežji. Uveljavljen je proces, ki zagotavlja redno oskrbovanje mobilne opreme z varnostnimi posodobitvami (proces OTA). Uporabljajo se ustrezne tehnologije za odkrivanje oz. preprečevanje napadov na omrežje podjetja (Intranet) (npr. sistemi za zaznavanje vdorov (Intrusion Detection System)). Zaposleni so ves čas obveščeni o nevarnostih in tveganjih.

Za zaščito aplikacij se uporabljajo nekateri standardni ukrepi:

pomembne aplikacije so z ustreznimi mehanizmi preverjanja pristnosti in odobritve zaščitene pred nepooblaščenim dostopom. Za gesla veljajo ustrezne specifikacije (skladne z najsodobnejšo tehniko) (dolžina, kompleksnost, trajanje veljavnosti gesla itd.). Za aplikacije, ki zahtevajo posebno zaščito, se uporabljajo zelo strogi mehanizmi preverjanja pristnosti (npr. tokenizacija, PKI). Večkraten napačen vnos kombinacije uporabniškega imena/gesla povzroči (začasno) blokado uporabniškega imena. Podatki, ki se uporabijo v ustreznem postopku, so v šifrirani obliki shranjeni na mobilnem nosilcu podatkov. Opravljeni dostopi in poskusi dostopa do aplikacij se beležijo. Ustvarjeni podatki beleženja se za ustrezen čas (najmanj 90 dni) shranijo in preverjajo (z naključnim pregledom vzorcev).

Uporabniške pravice (za dostop) so zagotovljene z različnimi ukrepi, pri čemer so praviloma dodeljene eni določljivi osebi. Izdaja pravic je v pristojnosti upravljavca platforme in se redno preverja. Pravice dostopa se dodeljujejo izključno v skladu z določenim in dokumentiranim procesom. Spremembe glede pravic dostopa se opravljajo po načelu »štirih oči« in se dokumentirajo v spremenjeni različici dnevniške datoteke.

Za nadzorovanje oz. upravljanje dostopa se uporabljajo različni ukrepi: pravice dostopa se opredelijo in dokumentirajo v okviru načela vlog/pravic ter se dodelijo posameznim vlogam v skladu z zahtevami določene naloge. Za tehnične skrbnike so urejene posebne vloge/pravice (ki, če je tehnično mogoče, onemogočajo dostop do osebnih podatkov). Posebne vloge/pravice so urejene tudi za strokovno podporo (ne vključujejo pravic tehničnih skrbnikov).

Če je tehnično in organizacijsko mogoče, opredelitve ter dodelitve vlog/pravic ne opravljajo iste osebe. Poleg tega se izvajata po postopku (odobritve), ki onemogoča posege, in sta časovno omejeni. Neposreden dostop do podatkovnih zbirk brez uporabe načela vlog/pravic je omogočen le pooblaščenim skrbnikom podatkovnih zbirk. Uporaba zasebnih nosilcev podatkov je urejena s posebnim predpisom ali pa je v celoti prepovedana. Veljajo obvezujoči predpisi glede dostopa do podatkov pri zunanjih vzdrževalnih delih, oddaljenih vzdrževalnih delih in delu na daljavo. Za uničenje/odstranjevanje dokumentov in nosilcev podatkov na način, ki spoštuje varstvo podatkov (npr. drobilnik, smetnjak za zaupne dokumente), se pooblasti zanesljivo podjetje za odstranjevanje odpadkov.

Načelo vlog/pravic se redno prilagaja spreminjajočim se strukturam organizacije dela (npr. nove vloge) in dodeljene pravice/vloge se redno preverjajo (npr. s strani nadrejenih) ter po potrebi prilagodijo oz. odvzamejo.

Redno se izvaja centralni nadzor nad dodeljenimi standardnimi profili. Posegi, s katerimi se opravijo spremembe (zapisi, izbrisi), se zabeležijo in ustvarjeni podatki beleženja se za ustrezen čas (najmanj 90 dni) shranijo ter preverjajo (z naključnim pregledom vzorcev).

Kot splošni ukrepi za zaščito posredovanja se uporabljajo različni standardni ukrepi:

osebe, zadolžene za posredovanje, se predhodno seznanijo z varnostnimi ukrepi, ki jih je treba izvesti. Predhodno se določi krog prejemnikov, s čimer se omogoči ustrezen nadzor (preverjanje pristnosti). Celotni proces posredovanja podatkov je določen in dokumentiran, zabeleži oz. dokumentira pa se tudi izvedba konkretnega posredovanja (npr. potrdilo o prejemu, potrdilo o plačilu). Osebe, zadolžene za posredovanje, predhodno preverijo verodostojnost, celovitost in pravilnost.

Pred izvedbo konkretnega prenosa podatkov se preveri naslov prejemnika (npr. e-poštni naslov). Prenos podatkov prek interneta se izvede v šifrirani obliki (npr. s šifriranjem datotek). Integriteta posredovanih podatkov se, če je tehnično mogoče, zagotovi s podpisom (digitalni podpis). Elektronska potrdila o prejemu se ustrezno arhivirajo. Neželeni prenosi podatkov po internetu se preprečijo z ustreznimi tehnologijami (npr. s posredniškim strežnikom, požarnim zidom).

Poleg tega se uporabljajo naslednji standardni ukrepi za izvedbo pravila ločevanja:

Veljajo obvezujoči predpisi glede omejitve namena obdelave za upoštevanje pravila ločevanja. Podatki, zbrani za določene namene, se hranijo ločeno od podatkov, zbranih za druge namene. Uporabljeni IT-sistemi omogočajo ločeno hrambo podatkov (s funkcijo za obravnavo več strank ali koncepti dostopa). Ločevanje podatkov se izvaja v testnih in produktivnih sistemih. Pri psevdonimiziranih podatkih se šifrirni mostič, ki omogoča ponovno prepoznavnost, shrani ločeno. Izvajalec pri obdelavi podatkov ali prenosu funkcij podatke različnih naročnikov obdeluje ločeno. Zasnova obstoječih konceptov vlog/pravic omogoča logično ločevanje obdelovanih podatkov.

4. Zagotavljanje integritete

Za beleženje vnosov se uporabljajo različni standardni ukrepi:

Spremembe pravic dostopa in vse skrbniške dejavnosti se zabeležijo. Zabeležijo se pisni posegi (vnosi, spremembe, izbrisi) in spremembe v podatkovnih poljih (npr. vsebina novo vnesenega ali spremenjenega zapisa). Zabeležijo se prenosi in prijave.

Dokumentacija, uporabljena za evidentiranje, se dokumentira in arhivira za zagotovitev sledljivosti vnosov. Zabeležijo se datum in čas, uporabnik, vrsta aktivnosti, aplikacijski program in zaporedna številka zapisa. Nastavitve beleženja se dokumentirajo.

Dnevniške datoteke se dajo na voljo izključno za branje. Krog oseb, ki imajo pravico dostopa do dnevniških datotek, je zelo omejen (npr. na skrbnika, nadzornika za varstvo podatkov in revizorja). Dnevniške datoteke se

za določen čas (npr. 1 leto) shranijo in nato izbrišejo v skladu z zahtevami o varstvu podatkov. Dnevniške datoteke se redno samodejno vrednotijo. Če je mogoče, se vrednotenja izvajajo v psevdonimizirani obliki.

5. Zagotavljanje razpoložljivosti

Arhitektura je zaščitena pred izgubo podatkov z replikacijskimi mehanizmi znotraj platforme Amazon Web Services. Poleg tega se za zaščito objektov uporabljajo naslednji standardni ukrepi Amazon Web Services:

Izvajajo se protipožarni ukrepi (npr. protipožarna vrata, javljalniki dima, protipožarne stene, prepoved kajenja). Računalniška oprema je zaščitena pred poplavami (npr. računalniški prostor v 1. nadstropju, detektor vode). Izvajajo se ukrepi za zaščito pred tresenjem (npr. računalniški prostor ni v bližini glavnih cest, železniških tirov, strojnic). Računalniška oprema je zaščitena pred elektromagnetnimi polji (npr. jeklene plošče na zunanjih stenah). Izvajajo se ukrepi za zaščito pred vandalizmom in tatvinami (gl. nadzor dostopa). Računalniška oprema je v klimatiziranih prostorih (temperaturo in vlago v zraku uravnava klimatska naprava). Računalniška oprema ima prenapetostno zaščito pred prenapetostnimi konicami. Izvajajo se ukrepi za zagotavljanje nemotenega in neprekinjenega tokovnega napajanja (npr. naprave za neprekinjeno napajanje, generatorji za zasilno napajanje).

Podatki so zaščiteni z rednim varnostnim kopiranjem znotraj platforme Amazon Web Services. Koncept varnostnega kopiranja je dokumentiran ter se redno preverja in posodablja. Nosilci varnostnih kopij so zaščiteni pred nepooblaščenim dostopom. Programi, ki se uporabljajo za varnostno kopiranje, so v skladu z najnovejšimi standardi kakovosti in se temu primerno redno posodabljajo. Urejen je dodaten računalniški center (stran od kraja obdelave), ki v primeru katastrofe omogoča nadaljevanje obdelave podatkov. Različni ukrepi za preverjanje razpoložljivosti so dokumentirani v načrtu Amazon Web Services za obvladovanje izrednih razmer.

Pred oddajo naročila za obdelavo podatkov se izvajalec temeljito preveri v skladu z določenimi merili (tehnični in organizacijski ukrepi). V ta namen se zlasti zahteva podroben opis tehničnih/organizacijskih ukrepov za varstvo podatkov (izpolnitev vprašalnika ali koncept varstva podatkov), ki se tudi preverijo. Glede na količino in občutljivost obdelanih podatkov se takšno preverjanje po potrebi opravi tudi na samem mestu pri izvajalcu. Pri izbiri izvajalcev se upoštevajo ustrezni certifikati (npr. ISO 27001). Ugotovitev primernosti izvajalca se ustrezno in razumljivo dokumentira.

Za potrditev pogodbenega razmerja naročnik in izvajalec skleneta pogodbo o obdelavi podatkov. V pogodbi so natančno in v pisni obliki opredeljene pristojnosti ter odgovornosti in obveznosti obeh strank. Če ima kateri od pooblaščenih izvajalcev storitev sedež zunaj EU oz. EGP, se uporabijo standardne pogodbene klavzule, ki se uporabljajo v Evropski uniji. Pogodbeno je določeno, da sme izvajalec obdelovati podatke izključno v okviru navodil naročnika. Če izvajalec meni, da katero od naročnikovih navodil krši predpise o varstvu podatkov, mora o tem nemudoma obvestiti naročnika. Da se zagotovi spoštovanje pravic posameznikov, na katere se nanašajo osebni podatki, se v pogodbi o obdelavi podatkov določi, da mora izvajalec zagotavljati ustrezno podporo naročniku, če je to na primer potrebno v primeru zagotavljanja informacij osebam, na katere se nanašajo osebni podatki.

V nadaljevanju obdelave podatkov naročnik preverja rezultate izvajalčevega dela glede oblike in vsebine. Preverja se tudi upoštevanje tehničnih in organizacijskih ukrepov, ki jih je sprejel izvajalec. To se potrjuje predvsem s predložitvijo aktualnih potrdil ali certifikatov oz. z dokazilom o izvedenih varnostnih IT-revizijah ali revizijah varstva podatkov. Če se najamejo podizvajalci, se v skladu s pogodbo ustrezno preverjajo tudi ti.

6. Zagotavljanje odpornosti sistemov

Infrastruktura v oblaku Amazon Web Services je bila oblikovana kot eno najprožnejših in najvarnejših računalniških okolij v oblaku. Zasnovana je bila za optimalno razpoložljivost pri popolni ločenosti strank. Zagotavlja platformo, ki je izredno nadgradljiva in varna za uporabo ter omogoča strankam, da aplikacije in vsebine po potrebi hitro in varno uporabljajo povsod po svetu. Storitve Amazon Web Services so vsebinsko neodvisne, saj vsem strankam zagotavljajo enako visoko raven varnosti, ne glede na vrsto vsebin ali geografsko regijo, v kateri so vsebine shranjene.

Visoko zaščiteni prvorazredni računalniški centri Amazon Web Services uporabljajo najsodobnejše ukrepe elektronskega nadzora in sisteme večstopenjskega nadzorovanja dostopa. V računalniških centrih je nenehno prisotno usposobljeno varnostno osebje in dostop je strogo zavarovan z načelom najmanjših pravic ter omogočen izključno skrbnikom sistemov.

7. Postopki za ponovno zagotovitev razpoložljivosti osebnih podatkov po fizičnem ali tehničnem incidentu

Računalniški centri Amazon Web Services so vzpostavljeni v različnih regijah po svetu in so med seboj povezani. Vsi računalniški centri so na voljo na spletu in zagotavljajo storitve strankam; noben računalniški center ni izklopljen. V primeru izpada samodejni procesi preusmerijo pretok podatkov strank proč od prizadetih območij. Ključne aplikacije so zagotovljene v konfiguraciji N+1, tako da je pri izpadu računalniškega centra na voljo dovolj zmogljivosti, da se obremenitev pretoka podatkov enakomerno porazdeli po preostalih lokacijah.

Amazon Web Services zagotavlja prilagodljivost za namestitev instanc in shranjevanje podatkov v več geografskih regijah ter prek več območij razpoložljivosti znotraj posameznih regij. Vsako območje razpoložljivosti je bilo razvito kot neodvisno območje v primeru izpada. To pomeni, da so območja razpoložljivosti fizično porazdeljena po tipičnih mestni regijah in se na primer nahajajo na območjih z nizkim tveganjem poplav (glede na regijo obstajajo različne kategorizacije poplavnih območij). Vsa območja razpoložljivosti imajo samostojno neprekinjeno tokovno napajanje in zasilne generatorje na kraju samem ter so poleg tega napajane iz različnih električnih omrežij neodvisnih dobaviteljev električne energije, s čimer se minimizirajo posamična mesta izpadov. Vsa območja razpoložljivosti so redundantno povezana s ponudniki Tier-1-Transit.

Ekipa podjetja Amazon za obvladovanje incidentov uporablja običajne panožne diagnostične postopke za pospešeno odpravljanje incidentov, ki so ključni za poslovanje. Operativno osebje je ves čas, tj. sedem dni na

teden in 365 dni na leto, na voljo za pomoč pri odkrivanju napak ter obvladovanju njihovih posledic in njihovem odpravljanju.

8. Postopki rednega preverjanja, vrednotenja in ocenjevanja učinkovitosti tehničnih in organizacijskih ukrepov

Smernice in navodila, ki se uporabljajo v podjetju, oz. upoštevani standardi za varnost informacij se uporabljajo tudi v povezavi z vzpostavitvijo in delovanjem platforme RIO. Na voljo so operativne funkcije za varstvo podatkov in varnost informacij (nadzornik za varstvo podatkov in odgovorni za informacijsko varnost). Zaposleni se zavežejo, da bodo ohranjali tajnost podatkov, ter se prek brošur, letakov, intranetnih navodil itd. poučijo o ukrepih za varstvo podatkov oz. varnostnih IT-ukrepih.

Z revizijami se preverja, ali se v notranjih procesih upoštevajo tehnični in organizacijski ukrepi za varstvo podatkov, varnost informacij in zaščito podatkov.

Postopki obdelave in ukrepi za varstvo podatkov se dokumentirajo v obliki seznama dejavnosti obdelave. Redno se izvaja (notranje in zunanje) preverjanje učinkovitosti ukrepov.