Pasūtījuma datu apstrādes līgums (atbilstīgi VDAR 28. pantam)

starp

lietotāju (kā ir definēts galvenajā līgumā)

(tālāk tekstā "**Pasūtītājs**")

un

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

(tālāk tekstā "**Izpildītājs**")
(Pasūtītājs un Izpildītājs tālāk tekstā atsevišķi – "**Puse**", abi kopā – "**Puses**").

Preambula

(A) Šis pasūtījuma datu apstrādes līgums (tālāk tekstā "**Līgums**") attiecas uz visām darbībām, kuru laikā Izpildītājs saskaras ar Pasūtītāja, trešo pušu vai citu datu subjektu personas datiem (kā ir definēts 1.5. punktā), kas ir saistīti ar 2. punktā aprakstītajām darbībām, kas izriet no platformas izmantošanas vispārīgajiem noteikumiem un atbilstīgi tiem noslēgtajiem atsevišķajiem līgumiem par papildu pakalpojumiem (tālāk tekstā "**Galvenais līgums**").

(B) Saskaņā ar Līgumu Pasūtītājs darbojas kā pārzinis un Izpildītājs – kā pasūtījuma datu apstrādātājs, veicot pasūtījuma datu apstrādi saskaņā ar VDAR 28. pantu (kā ir definēts tālāk).

Tādēļ Puses vienojas par sekojošo:

1 Definīcijas un interpretācija

1.1 "**Eiropas tiesības**" ir Eiropas Savienības piemērojamās tiesības, tagadējo Eiropas Savienības dalībvalstu piemērojamie likumi un tās valsts piemērojamie likumi, kura vēlāk kļūs par Eiropas Savienības dalībvalsti.

1.2 "**Eiropas datu aizsardzības tiesības**" ir Eiropas Savienības piemērojamās tiesības par personas datu apstrādi (it īpaši VDAR), tagadējo Eiropas Savienības dalībvalstu piemērojamie likumi par personas datu apstrādi (it īpaši BDSG attiecīgajā brīdī spēkā esošajā redakcijā) un tās valsts piemērojamie likumi par personas datu apstrādi, kura vēlāk kļūs par Eiropas Savienības dalībvalsti.

1.3 "**VDAR**" ir "EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula)".

1.4 "**BDSG**" ir Vācijas Federālais Datu aizsardzības likums.

1.5 Jēdziens "**personas dati**" tiek lietots nozīmē, kas ir definēta BDSG un VDAR.

2 Datu apstrādes priekšmets/Pasūtītāja pienākumi

2.1 Šis Līgums nosaka Pušu pienākumus Pasūtītāja personas datu apstrādē, ko Izpildītājs veic saskaņā ar 1. pielikumā minēto Galveno līgumu.

2.2 Apstrādes priekšmets un ilgums, apstrādes veids un nolūks, personas datu veids, datu subjektu kategorijas un pārziņa pienākumi un tiesības izriet no Līguma 1. pielikuma un Galvenā līguma pakalpojumu apraksta.

2.3 Pasūtītājs ir pārzinis atbilstīgi VDAR un nodrošina, ka ir atļauts apstrādāt datu subjektu (vadītāja un citu iespējamo personu) personas datus. Attiecīgi Pasūtītājs jo īpaši pilda savu pienākumu sniegt visaptverošu informāciju un nodrošina, ka personas datu apstrāde balstās uz datu aizsardzības tiesību juridisku pamatu (piemēram, darba līguma noslēgšana, apstrādes ierobežošana darba tiesisko attiecību nolūkos).

3 Izpildītāja pienākumi

3.1 Izpildītājs apstrādā Pasūtītāja personas datus tikai 1. pielikumā minētajos nolūkos un saskaņā ar Galveno līgumu, kā arī pasūtījuma laikā un saskaņā ar 1. pielikumā dokumentētajiem Pasūtītāja norādījumiem; Izpildītājs saskaņā ar Līgumu neapstrādā personas datus citos nolūkos. Šis noteikums neattiecas uz apstrādi ārpus Līguma nosacījumiem savām vajadzībām saskaņā ar Galvenā līguma 8.3.4. punktu. Personas datu kopiju un dublikātu sagatavošana bez Pasūtītāja ziņas ir aizliegta. Izņēmums ir drošības kopijas, ja tās ir vajadzīgas, lai nodrošinātu atbilstīgu datu apstrādi, kā arī dati, kas ir vajadzīgi, lai tiktu ievērotas tiesību aktos noteiktās glabāšanas prasības.

3.2 Pēc apstrādes pakalpojumu sniegšanas Izpildītājam pēc Pasūtītāja izvēles ir jānodod tam un/vai atbilstīgi datu aizsardzības prasībām jāizdzēš visi Pasūtītāja personas dati, ja tas nav pretrunā tiesību aktos noteiktajam glabāšanas termiņam un Izpildītājs tos neapstrādā savām vajadzībām ārpus Līguma nosacījumiem saskaņā ar Galvenā līguma 8.3.4. punktu. Tas pats attiecas uz testa un izbrāķēto materiālu. Pēc pieprasījuma Pasūtītājam ir rakstiski, norādot datumu, jāapstiprina, ka dati ir pilnībā izdzēsti vai nodoti viņam.

3.3 Ja to paredz pakalpojumu apjoms, Izpildītājs sniedz Pasūtītājam atbalstu datu subjektu tiesību nodrošināšanā (piekļuve, labošana, iebilšana, dzēšana) pēc attiecīga Pasūtītāja norādījuma.

3.4 Izpildītājs apstiprina, ka ir iecēlis uzņēmuma datu aizsardzības speciālistu, ja to nosaka tiesību akti (salīdzināt BDSG 38. pantu un VDAR 37. pantu).

3.5 Izpildītājs apņemas nekavējoties informēt Pasūtītāju par datu aizsardzības uzraudzības iestāžu pārbaužu rezultātiem, ja pārbaudes ir saistītas ar Pasūtītāja datu apstrādi. Konstatētos trūkumus Izpildītājs novērsīs atbilstošā termiņā un paziņos par to Pasūtītājam.

3.6 Izpildītājs un Pasūtītāja apstiprinātie apakšuzņēmēji apstrādā datus tikai Vācijas Federatīvās Republikas teritorijā, Eiropas Savienības dalībvalstī vai kādā citā Eiropas Ekonomikas zonas līgumvalstī. Lai datu apstrādi varētu veikt citā valstī (tālāk tekstā "**Trešā valsts**"), ir vajadzīga iepriekšēja skaidra Pasūtītāja piekrišana, turklāt tas ir atļauts tikai tad, ja ir izpildīti īpašie nosacījumi par datu eksportēšanu trešajās valstīs (salīdzināt VDAR 40. pantu un turpmākos pantus). Tad attiecīgi ir jāaizpilda 1. pielikums un jāpievieno papildu (līguma) dokumenti, ja ir vajadzīgs.

3.7 Izpildītājam ir jāiepazīstina darbu veikšanā iesaistītie darbinieki ar noteicošajiem datu aizsardzības noteikumiem un jāuzliek par pienākumu ievērot datu konfidencialitāti (salīdzināt VDAR 28. panta 3. punkta b) apakšpunktu), kā arī ar atbilstīgām darbībām ir jānodrošina, ka katrs darbinieks apstrādā personas datus tikai atbilstīgi pasūtītāja norādījumiem.

3.8 Izpildītājs uzrauga, lai regulāri visā Līguma darbības laikā tiktu ievēroti šajā Līgumā minētie datu aizsardzības noteikumi un dokumentētie Pasūtītāja norādījumi. Pēc pieprasījuma Pasūtītājam ir jāizsniedz pārbaužu rezultāti, ja tie attiecas uz Pasūtītāja datu apstrādi. Uzraudzības pasākumi ir aprakstīti datu aizsardzības koncepcijā, kas pēc pieprasījuma ir jāizsniedz Pasūtītājam.

3.9 Izpildītājs, ņemot vērā apstrādes veidu, un iespēju robežās palīdz Pasūtītājam ar atbilstīgiem tehniskiem un organizatoriskiem pasākumiem, kas nodrošina, ka Pasūtītājs var izpildīt savu pienākumu atbildēt uz pieprasījumiem par VDAR III nodaļā paredzēto datu subjekta tiesību īstenošanu. Pasūtītājs sedz izmaksas, kas Izpildītajam rodas saistībā ar šī pienākuma izpildi.

3.10 Izpildītājs palīdz Pasūtītājam nodrošināt VDAR 32. līdz 36. pantā minēto pienākumu izpildi, ņemot vērā apstrādes veidu un viņam pieejamo informāciju.

4 Tehniskie un organizatoriskie pasākumi datu drošības jomā

4.1 Izpildītājs veic atbilstīgus tehniskos un organizatoriskos datu aizsardzības pasākumus (salīdzināt VDAR 32. pantu). Izpildītāja pienākums ir jo īpaši īstenot Līguma 2. pielikumā noteiktos tehniskos un organizatoriskos pasākumus. Pasūtījuma saistību periodā Izpildītājam šie pasākumi ir jāpielāgo tehniskajai un organizatoriskajai attīstībai, nesamazinot aizsardzības līmeni. Par būtiskām izmaiņām ir jāvienojas rakstiski.

4.2 Pēc pieprasījuma Izpildītājs pierāda Pasūtītājam, ka tehniskie un organizatoriskie pasākumi tiešām ir ievēroti.

4.3 Izpildītāja pienākums ir dokumentēt datu apstrādi, lai Pasūtītājs varētu pierādīt, ka dati ir apstrādāti pienācīgi. Pierādījumu var iegūt arī apstiprinātā sertifikācijas procesā saskaņā ar VDAR 42. pantu.

5 Apakšuzņēmēji

5.1 Izpildītājam ir atļauts piesaistīt 1. pielikumā minētos apakšuzņēmējus.

5.2 Ar šo tiek atļauta arī citu apakšuzņēmēju piesaistīšana. Izpildītājam ir jāinformē Pasūtītājs par visām plānotajām izmaiņām, kas ir saistītas ar apakšuzņēmēju piesaistīšanu vai aizstāšanu; Pasūtītājs var iebilst pret plānotajām izmaiņām. Šī noteikuma izpratnē apakšuzņēmēja saistības nav pakalpojumi, kurus Izpildītājs no trešajām pusēm izmanto kā papildpakalpojumus, kas kalpo par atbalstu pasūtījumu izpildē. Pie šiem pakalpojumiem pieder, piemēram, telekomunikācijas pakalpojumi, uzkopšanas personāls, datu nesēju pārbaudīšana un utilizācija. Tomēr, lai nodrošinātu Pasūtītāja datu aizsardzību un drošību, arī izmantojot ārējo pakalpojumu sniedzēju pakalpojumus, Izpildītāja pienākums ir noslēgt atbilstošus un likumiem atbilstīgus līgumus un veikt kontroles pasākumus.

5.3 Ja Izpildītājs piesaista apakšuzņēmēju, Izpildītājam ir jānodrošina, ka tam, (i) noslēdzot līgumu starp apakšuzņēmēju un Izpildītāju vai (ii) izmantojot citus tiesību instrumentus saskaņā ar Eiropas Savienības datu aizsardzības tiesībām, tiek uzlikti tie paši datu aizsardzības pienākumi, kādi Izpildītājam ir saskaņā ar Līgumu. Izpildītājam ir jo īpaši jānodrošina, ka apakšuzņēmējs sniedz pietiekamas garantijas, ka atbilstīgie tehniskie un organizatoriskie pasākumi tiek veikti tā, lai personas datu apstrāde notiktu atbilstīgi VDAR prasībām. Pēc Pasūtītāja rakstiska pieprasījuma Izpildītājs sniedz Pasūtītājam informāciju par būtiskākajiem līguma noteikumiem un ar datu aizsardzību saistīto pienākumu izpildi attiecībā uz apakšuzņēmēja saistībām, vajadzības gadījumā ļauj ieskatīties attiecīgajos līgumos. Komerciālos nosacījumus Izpildītājs var nerādīt. Pasūtītāja pienākums ir nodrošināt iegūtās informācijas konfidencialitāti.

6 Kontroles tiesības

6.1 Pasūtītājam ir tiesības pašam kontrolēt šī Līguma saistību izpildi (ieskaitot dotos norādījumus) vai kontroles veikšanai iecelt piemērotu trešo personu.

6.2 Izpildītājs kontroles laikā sniedz Pasūtītājam atbilstošu atbalstu. Izpildītājs nodrošina piekļuvi datu apstrādes iekārtām un sniedz vajadzīgo informāciju.

6.3 Gadījumā, ja kontroles laikā tiek konstatēts, ka Izpildītājs neievēro šī līguma prasības un/vai Eiropas datu aizsardzības tiesības, un/vai apstrāde nav veikta saskaņā ar šī līguma prasībām un/vai Eiropas datu aizsardzības tiesībām, Izpildītājam ir jāveic visi koriģējošie pasākumi, kas nepieciešami, lai tiktu ievērotas šī līguma prasības un/vai Eiropas datu aizsardzības tiesības.

6.4 Izmaksa, kas Pasūtītājam rodas, veicot kontroli, sedz viņš pats. Segt izmaksas, kas Izpildītājam rodas, kad Pasūtītājs veic kontroli, viņš var pieprasīt Pasūtītājam, ja Pasūtītājs veic kontroli vairāk nekā reizi kalendārajā gadā.

6.5 Ja pie Izpildītāja vēlas veikt kontroli, tā ir savlaicīgi jāpiesaka un tā nedrīkst būtiski traucēt Izpildītāja uzņēmuma darbību.

7 Informēšanas pienākums

Izpildītājs nekavējoties informē Pasūtītāju, ja kāds no Pasūtītāja dotajiem norādījumiem pēc Izpildītāja domām ir pretrunā Eiropas datu aizsardzības tiesībām. Norādījumi, pret kuriem ir celti patiesi iebildumi, nav jāievēro, kamēr Pasūtītājs tos nav izmainījis vai skaidri apstiprinājis. Izpildītājam nav pienākuma pārbaudīt norādījumu materiāli tiesisko atbilstību.

Ja Izpildītājs datu apstrādē konstatē kļūdas vai nepilnības vai ir aizdomas par datu aizsardzības pārkāpumu (tālāk tekstā "**Atgadījums**"), viņš nekavējoties par to informē Pasūtītāju. Izpildītājam ir jādokumentē Atgadījums, ieskaitot visus lietas apstākļus, tā sekas un visus novēršanas pasākumus, un pēc Pasūtītāja pieprasījuma šī dokumentētā informācija ir nekavējoties rakstiski vai elektroniski jānodod Pasūtītājam.

8 Atbildība un atbrīvošana no atbildības

8.1 Izpildītājs atbild par zaudējumiem, kurus tas vai tā pārstāvis ir radījis tīši un/vai rupjas neuzmanības dēļ. Par zaudējumiem, kurus Izpildītājs vai tā pārstāvis ir radījis vienkāršas neuzmanības dēļ, Izpildītājs atbild tikai tādā gadījumā, ja ir pārkāpts galvenais pienākums. Galvenie pienākumi ir būtiskākie Līgumā noteiktie pienākumi, bez kuriem nav iespējama pienācīga līguma izpilde, un uz kuru izpildi Pasūtītājs ir paļāvies un drīkstēja paļauties. Vienkāršas neuzmanības gadījumā attiecībā uz galveno pienākumu pārkāpšanu atbildība aprobežojas ar tipiski paredzamiem zaudējumiem.

8.2 Pasūtītājs atbrīvo Izpildītāju no visām trešo personu (ieskaitot datu subjektu un/vai datu aizsardzības iestāžu) prasībām, zaudējumu atlīdzības un izdevumu segšanas, kas radušies no tā, ka Pasūtītājs ir pārkāpis šī Līguma noteikumus un/vai Eiropas datu aizsardzības tiesības; šis noteikums nav spēkā, ja Pasūtītājs nav vainīgs pārkāpuma izdarīšanā vai ja Izpildītājs ir līdzvainīgs pārkāpumā.

9 Darbības laiks

Šī Līguma darbības laiks atbilst Galvenā līguma darbības laikam. Ja kāda iemesla dēļ Galvenais līgums tiek izbeigts, automātiski tiek izbeigts arī šis Līgums. Tiesības lauzt Līgumu svarīga iemesla dēļ paliek spēkā.

10 Citi noteikumi

10.1 Samaksa par šajā Līgumā noteiktajiem Izpildītāja pakalpojumiem tiek veikta saskaņā ar Galvenajā līgumā aprakstītajiem atlīdzības noteikumiem.

10.2 Ja Pasūtītāja personas datu drošību pie Izpildītāja apdraud trešo pušu pasākumi (piemēram, apķīlāšana vai atsavināšana), maksātnespējas vai izlīguma process vai kāds cits līdzīgs notikums, Izpildītājam par to nekavējoties ir jāinformē Pasūtītājs.

10.3 Ja kāds no šī Līguma noteikumiem zaudē spēku, tas neietekmē pārējo noteikumu spēkā esamību. Ja kāds no noteikumiem zaudē spēku, Puses vienojas par citu noteikumu, kas materiālā un ekonomiskā ziņā atbilst Līguma mērķim.

10.4 Gadījumā, ja Lielbritānija izstāsies no Eiropas Savienības, Izpildītājs apņemas jau tagad noslēgt visas vienošanās un veikt visas darbības, kas ir nepieciešamas, lai līgumā noteiktā datu apstrāde, ievērojot datu aizsardzības tiesības, Lielbritānijā būtu atļauta jau no izstāšanās brīža. Ja izstāšanās brīdī nav pozitīva Eiropas Komisijas lēmuma par aizsardzības līmeņa pietiekamību, no šodienas skatpunkta tās ir standarta datu aizsardzības klauzulas saskaņā ar VDAR 46. panta 2. punkta c) apakšpunktu par personas datu nosūtīšanu pasūtījuma datu apstrādātajiem, kas veic uzņēmējdarbību Trešajās valstīs, kurās nav nodrošināts atbilstīgs aizsardzības līmenis.

Ja Izpildītājs nepilda šos pienākumus, Pasūtītājs ir tiesīgs Izpildītājam pieprasīt, ka no brīža, kad Lielbritānija ir izstājusies no Eiropas Savienības, attiecīgos pakalpojumus sniedz kāds saistīts uzņēmums vai attiecīgi uzņēmuma daļa, kura pastāvīgā mītne ir Eiropas Savienības teritorijā, neradot Pasūtītājam papildu izmaksas.

10.5 Šis pasūtījuma datu apstrādes līgums ir sagatavots 18 valodās; ja ir neatbilstības, prioritāra ir oriģinālā versija vācu valodā.

10.6 Šis Līgums ir pakļauts Vācijas Federatīvās Republikas likumiem, izņemot Konvenciju par starptautiskajiem preču pirkuma-pārdevuma līgumiem. Ekskluzīva jurisdikcija ir Minhenes (Vācija) tiesām.

10.7 Tālāk norādītie pielikumi ir Līguma sastāvdaļa:

1. pielikums – Pasūtījuma datu apstrādes apraksts
2. pielikums – Tehniskie un organizatoriskie pasākumi

1. PIELIKUMS – Pasūtījuma datu apstrādes apraksts

1 Galvenais līgums

Galvenais līgums šī Līguma pamatdaļas 2.1. punkta izpratnē ir "Platformas izmantošanas vispārīgie noteikumi".

Nosaukums / Puses: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19–21, 80807 München/**Lietotājs**

2 Pasūtījuma priekšmets un ilgums

Pasūtījuma priekšmets izriet no Galvenā līguma 1. punkta *(Priekšmets)* un 8. punkta *(Lietotāja dati un datu aizsardzība)*; pasūtījuma ilgums izriet no Galvenā līguma 7. punkta *(Līguma noslēgšana, termiņš un uzteikuma tiesības)*.

3 Datu apstrādes apjoms, veids un nolūks/datu apstrādes pasākumi

Personas datu apstrādes apjoms, veids un nolūks izriet no Galvenā līguma 8. punkta.

Detalizēts pasūtījuma priekšmeta, proti, tā apjoma, veida un nolūka, apraksts

Lai varētu sniegt Izpildītāja piedāvātos pakalpojumus (kā ir definēts Galvenajā līgumā), Izpildītājam no pieslēgtajiem transportlīdzekļiem vai mobilajām ierīcēm ir jāievāc Pasūtītāja personas dati (iespējams, arī no trešās puses, ar kuru lietotājs ir vienojies par trešo pušu pakalpojumiem, pārsūtītie personas dati) apjomā, kāds ir vajadzīgs, lai sniegtu pakalpojumus, jāpārsūta tie uz Izpildītāja platformu un tur jāsaglabā. Izpildītājs apstrādā platformā saglabātos datus apjomā, kāds ir vajadzīgs, lai sniegtu pakalpojumus (piemēram, lai analizētu un izvērtētu vadītāju braukšanas īpašības, kā arī pieslēgtā transportlīdzekļa vai mobilās ierīces lietojumu, izmantojot personas datus, un sagatavotu Pasūtītājam īpaši viņam piemērotus piedāvājumus, piemēram, vadītāja apmācības, aprīkojuma detaļas, kā arī efektivitātes uzlabošanas ieteikumus, balstoties uz šiem datiem). Precīzs apjoms, veids un nolūks tiek noteikts papildus noslēdzamajos atsevišķajos līgumos.

4 Datu subjektu loks (datu subjektu kategorijas)

Pasūtījuma datu apstrāde attiecas uz šādu personu loku:

- **vadītāji un citi darbinieki** (Pasūtītāja sabiedrības darbinieki), piemēram, darba ņēmēji, praktikanti, kandidāti, bijušie darbinieki*;*
- **vadītāji**, kas nav darbinieki;
- iekrāvēju/izkrāvēju vai citu Pasūtītāja sadarbības partneru **kontaktpersonas**;
- **koncerna darbinieki** (cita Pasūtītāja grupas uzņēmuma darbinieki).

5 Personas datu veids

Pasūtījuma datu apstrādē ir iekļauti šādi personas datu veidi:

- vadītāja vārds, uzvārds un vadītāja identifikācijas numurs;
- transportlīdzekļa identifikācijas numurs;
- atrašanas vietas dati;
- dati par vadīšanas un atpūtas laikiem;
- dati par braukšanas īpašībām;
- pieslēgtā transportlīdzekļa stāvokļa dati;
- autopiekabes stāvokļa dati;
- uzbūves un piebūves aprīkojuma, agregātu un citu transportlīdzekļa detaļu stāvokļa dati;
- savienoto IOT ierīču stāvokļa dati;
- mobilo ierīču stāvokļa dati;
- kravas dati;
- pasūtījuma dati; un
- iekrāvēju/izkrāvēju vai citu Pasūtītāja sadarbības partneru kontaktpersonu kontaktinformācija.

6 Dokumentētie norādījumi

Pasūtītājs dod norādījumu Izpildītājam apstrādāt personas datus atbilstīgi Galvenā līguma 8. punktam. Apstrādē ir ietvertas arī tālāk minētās darbības.

- Personas dati no pieslēgtā transportlīdzekļa vai mobilās ierīces tiek pārsūtīti uz mākonī izvietoto Izpildītāja platformu un tur saglabāti.
- Saskaņā ar Līgumu personas dati tiek apstrādāti tikai tad, ja tas ir vajadzīgs, lai izpildītu Galvenā līguma saistības; šis noteikums nemaina Galvenā līguma 8.3.4. punktu.
- Izpildītājs nosūta personas datus trešajai pusei (kā ir definēts Galvenajā līgumā), ja šāda nosūtīšana trešajai pusei ir vajadzīga, lai tā Pasūtītājam varētu sniegt savus pakalpojumus (kā ir definēts Galvenajā līgumā).
- Izmantojot personas datus, Izpildītājs analizē un izvērtē vadītāju braukšanas īpašības, kā arī pieslēgtā transportlīdzekļa lietojumu un sagatavo Pasūtītājam īpaši viņam piemērotus piedāvājumus, piemēram, vadītāja apmācības, aprīkojuma detaļas, kā arī efektivitātes uzlabošanas ieteikumus, balstoties uz šiem datiem.

7 Apstrādes vieta

- Vācija.
- Apvienotā Karaliste, ja dati tiek apstrādāti Eiropas Savienībā IT viesošanas un/vai IT atbalsta nolūkos un ir noslēgti attiecīgie pasūtījuma datu apstrādes līgumi.

- Ja Izpildītājs IT viesošanas un/vai IT atbalsta nolūkos izmanto apakšuzņēmējus ārpus Eiropas Savienības (skatīt šī 1. pielikuma 8. punktu), personas datu tālāknodošana notiek, pamatojoties uz līguma standartklauzulām/standarta datu aizsardzības klauzulām, kas ir noslēgtas starp Izpildītāju un apakšuzņēmēju un nosaka personas datu nosūtīšanu pasūtījuma datu apstrādātājiem Trešajās valstīs atbilstīgi VDAR 46. panta 2. punkta c) apakšpunktam.

8 Apakšuzņēmēji

Izpildītājs izmanto šādus apakšuzņēmējus (kuri, ja nepieciešams, var piesaistīt vēl citus apakšuzņēmējus):

Nr.	Apakšuzņēmējs (firma, adrese, kontaktpersona)	Apstrādātās datu kategorijas	Apakšuzņēmēja apstrādes darbības/datu apstrādes nolūks
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Visi personas dati no platformas, kas ir saistīti ar pārdošanas daļu (tas ir, kur klients var reģistrēties platformā un veikt pasūtījumus)	Platformas viesošana
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Visi personas dati no platformas, kas ir saistīti ar pārdošanas daļu (tas ir, kur klients var reģistrēties platformā un veikt pasūtījumus)	IT atbalsts saistībā ar platformu
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 USA https://aws.amazon.com/de/compliance/contact/	Visi citi lietotāja personas dati, kas no transportlīdzekļa tiek nosūtīti Izpildītājam	Platformas viesošana/IT atbalsts saistībā ar platformas viesošanu
4	Iespējams turpmāk Nr. 3 vietā Amazon Webservices (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 USA https://aws.amazon.com/de/compliance/contact/	Visi citi lietotāja personas dati, kas no transportlīdzekļa tiek nosūtīti Izpildītājam	Platformas viesošana
5	MAN Service und Support GmbH Dachauer Straße 667 80995 München	Visi personas dati, kas ir vajadzīgi, lai apstrādātu klientu pieprasījumu ar 1. un 2. līmeņa atbalstu	1. līmeņa atbalsts

	Deutschland		
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 USA	Visi personas dati, kas ir vajadzīgi, lai apstrādātu rēķinu sagatavošanu/pasūtījumu noformēšanu	Platformas viesošana (EU Tenant – Gehosted by Amazon Web Services (EU) – skatīt 4. punktu
7	MAN Truck & Bus AG Dachauer Str. 667 80995 München Deutschland	Visi citi lietotāja personas dati, kas no pieslēgtā transportlīdzekļa un/vai mobilās ierīces tiek nosūtīti Izpildītājam	Platformas viesošana
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Deutschland	Visi citi lietotāja personas dati, kas no TBM1/2 transportlīdzekļa tiek nosūtīti Izpildītājam	Platformas viesošana
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Sverige	Visi citi lietotāja personas dati, kas no transportlīdzekļa tiek nosūtīti Izpildītājam	Platformas viesošana
10	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hannover Deutschland	Visi citi lietotāja personas dati, kas no transportlīdzekļa tiek nosūtīti Izpildītājam	Platformas viesošana

2. PIELIKUMS – Tehniskie un organizatoriskie pasākumi
Tehniskie un organizatoriskie pasākumi, kas jāveic Izpildītājam, lai nodrošinātu riskam atbilstošu aizsardzības līmeni, ir aprakstīti RIO platformas datu aizsardzības koncepcijā, un tie ir:

1. Pseidonimizācija

Ja personas dati tiek izmantoti izvērtēšanas nolūkos, kuru var veikt arī ar pseidonimizētiem datiem, tiek izmantotas pseidonimizācijas metodes. Šajā gadījumā jau iepriekš katram datu laukam tiek noteikts, vai to vajag pseidonimizēt, jo tas varētu ļaut identificēt personu. Pseidonimizācijas atslēgas tiek saglabātas "datu seifā" ("Data Safe"), kuram piekļuve ir maksimāli ierobežota.

2. Šifrēšana

Mobilās galiekārtas šifrētā veidā komunicē ar galapunktu, izmantojot individuālu ierīces sertifikātu. Dati šifrētā veidā tiek transportēti tālāk RIO platformā ("Ubiquitous encryption" vai "encryption everywhere").

3. Konfidencialitātes nodrošināšana

Visiem darbiniekiem tiek prasīts neizpaust konfidenciālu informāciju un tiem ir rakstiski jāapņemas ievērot datu konfidencialitāti.

Izmantoto IT infrastruktūru nodrošina ar Amazon Web Services (tālāk tekstā "AWS") mākoņpakalpojumu (IaaS & PaaS). Piekļuves kontroli nodrošina AWS datu centra operators: augstas drošības AWS skaitļošanas centri izmanto augstāko tehnoloģiju elektroniskās uzraudzības pasākumus un vairāku līmeņu piekļuves kontroles sistēmas. Skaitļošanas centros visu diennakti strādā apmācīti drošības speciālisti, turklāt piekļuve tiek atļauta tikai pēc mazu tiesību principa un tikai sistēmas administrācijas nolūkos.

Piekļūt aparatūras komponentiem (klientdatoriem) uzņēmumā TB Digital Services GmbH var saskaņā ar spēkā esošajiem, katram atsevišķam gadījumam atbilstošiem standarta pasākumiem. Tie ir, piemēram, ieejas kontroles iekārtas (turniketi), videonovērošanas iekārtas, signalizācijas un/vai apsardze, elektroniski vai mehāniski aizsargātas durvis, pret ielaušanos aizsargātas ēkas, dokumentētas piekļuves tiesības (apmeklētāji, ārējie speciālisti) vai deklarētas drošības zonas.

Piekļuves kontroles ietver ierīču aizsardzības, tīkla aizsardzības un programmu aizsardzības pasākumus.

Lai transportlīdzeklī nodrošinātu ierīču aizsardzību, ir ieviesti dažādi pasākumi: Mobilās galiekārtas ir iebūvētas transportlīdzeklī un ir aprīkotas ar drošas palaišanas tehnoloģiju Secure Boot, kas nozīmē, ka nevar ielādēt un palaist svešu operētājsistēmu. Mobilās galiekārtas šifrētā veidā komunicē ar galapunktu, izmantojot individuālu ierīces sertifikātu. Dati šifrētā veidā tiek transportēti tālāk RIO platformā ("Ubiquitous encryption" vai "encryption everywhere"). Galiekārtām vienmēr ir jaunākā drošības versija, jo regulāri tiek instalētas drošības atjauninājumu pakotnes (ielāpu pārvaldība).

Lai nodrošinātu tīkla aizsardzību, ir ieviesti dažādi standarta pasākumi: Ir ieviestas piemērotas (tehnikas līmenim atbilstošas) paroles prasības (paroles garums, sarežģītība, derīguma termiņš u. c.). Ja lietotāja identifikators/paroles kombinācija vairākkārt tiek ievadīta nepareizi, lietotāja identifikators uz laiku tiek bloķēts. Uzņēmuma tīklu pret nedrošiem publiskiem tīkliem aizsargā ugunsmūris. Ir ieviests process, kas palīdz regulāri apgādāt mobilās ierīces ar drošības atjauninājumu pakotnēm (OTA process). Lai atklātu vai novērstu uzbrukumus uzņēmuma tīklam (iekštīklam), tiek izmantotas atbilstošas tehnoloģijas (piem., ielaušanās atklāšanas sistēma). Darbiniekiem regulāri tiek atgādināts par bīstamību un riskiem.

Lai nodrošinātu programmu aizsardzību, ir ieviesti daži standarta pasākumi:

attiecīgās programmas pret neatļautu piekļuvi aizsargā atbilstoši autentifikācijas un autorizācijas mehānismi. Ir ieviestas piemērotas (tehnikas līmenim atbilstošas) paroles prasības (paroles garums, sarežģītība, derīguma termiņš u. c.). Programmām, kurām nepieciešama īpaša aizsardzība, tiek izmantoti spēcīgāki autentifikācijas mehānismi (piem., Token, PKI). Ja lietotāja identifikators/paroles kombinācija vairākkārt tiek ievadīta nepareizi, lietotāja identifikators uz laiku tiek bloķēts. Attiecīgajā procesā izmantotie dati šifrētā formā atrodas mobili lietojamā datu nesējā. Piekļūšana programmām un piekļūšanas mēģinājumi tiek dokumentēti. Ģenerētās protokola datnes tiek uzglabātas noteiktu laika periodu (vismaz 90. dienas) un (izlases veidā) pārbaudītas.

Lietotāja (pieejas un piekļuves) tiesības tiek nodrošinātas, veicot dažādus pasākumus, un tās ir piesaistītas kādai konkrētai personai. Piekļuves tiesības piešķir platformas pārzinis un tās regulāri tiek pārbaudītas. Piekļuves tiesību piešķiršana notiek tikai atbilstīgi definētam un dokumentētam procesam. Piekļuves tiesību mainīšana notiek tikai pēc četru acu principa, un šīs izmaiņas tiek dokumentētas attiecīgās versijas žurnālfailā.

Lai nodrošinātu piekļuves kontroli un vadību, ir ieviesti dažādi pasākumi: piekļuves tiesības tiek noteiktas un dokumentētas lomu un tiesību koncepcijā un atbilstoši uzdevumu prasībām piesaistītas attiecīgajai lomai. Tehniskajiem administratoriem ir izveidotas speciālas lomas un tiesības (ja tehniski iespējams, viņi nevar nodrošināt piekļuvi personas datiem). Profesionālā atbalsta speciālistiem ir izveidotas speciālas lomas un tiesības (nav iekļautas tehniskā administratora tiesības).

Ja tehniski un organizatoriski iespējams, tad lomu un tiesību definēšanu un to piesaistīšanu neveic vienas un tās pašas personas, un tas notiek saskaņā ar auditā pārbaudītu (apstiprināšanas) procesu un noteiktā termiņā. Tieši piekļūt datubāzei, apejot lomu un tiesību koncepciju, var tikai autorizēti datubāzes administratori. Ir noteikums par privāto datu nesēju izmantošanu, respektīvi, privāto datu nesēju izmantošana ir aizliegta. Eksistē saistoši noteikumi attiecībā uz piekļūšanu datiem, kad tiek veiktas ārējās apkopes, attālinātās apkopes un attālinātais darbs. Dokumentu un datu nesēju iznīcināšana un utilizācija notiek atbilstīgi datu aizsardzības noteikumiem (piem., smalcinātājā, slēgtā datu konteinerā), un to veic uzticami atkritumu apsaimniekošanas uzņēmumi.

Lomu/tiesību koncepcija regulāri tiek pielāgota mainīgajām darba organizācijas struktūrām (piemēram, jaunas lomas) un piesaistītās lomas/tiesības tiek regulāri pārbaudītas (to dara, piemēram, uzņēmuma vadītājs) un attiecīgi pielāgotas vai atņemtas, ja ir vajadzīgs. Piešķirtos standarta profilus regulāri centralizēti pārbauda.

Piekļuves ar izmaiņu veikšanas tiesībām (rakstīšana, dzēšana) tiek protokolētas, un ģenerētās protokola datnes tiek glabātas noteiktu laika periodu (vismaz 90 dienas) un (izlases veidā) pārbaudītas.

Lai nodrošinātu datu tālāknodošanu, ir ieviesti dažādi standarta pasākumi:

Personas, kas ir pilnvarotas veikt tālāknodošanu, jau iepriekš tiek iepazīstinātas ar veicamajiem aizsardzības pasākumiem. Saņēmēju loks tiek noteikts jau iepriekš, lai varētu veikt atbilstošu kontroli (autentifikāciju). Viss datu tālāknodošanas process ir noteikts un dokumentēts, arī konkrēto datu tālāknodošana tiek protokolēta, respektīvi, dokumentēta (piemēram, saņemšanas apstiprinājums, kvīts). Personas, kas ir pilnvarotas nodot datus, vispirms veic ticamības, pilnīguma un pareizības pārbaudi.

Pirms konkrēto datu nosūtīšanas tiek pārbaudīta saņēmēja adrese (piem., e-pasta adrese). Datu nosūtīšana internetā notiek šifrētā formā (piem., datnes šifrēšana). Ja tehniski iespējams, tad tālāknodoto datu integritāte tiek panākta, izmantojot parakstīšanas metodes (elektronisko parakstu). Elektroniskie saņemšanas apstiprinājumi tiek arhivēti atbilstošā formā. Nevēlama datu pārsūtīšana internetā tiek novērsta ar atbilstošām tehnoloģijām (piem., Proxy, Firewall).

Lai varētu ievērot nodalīšanas principu, ir ieviesti šādi standarta pasākumi:

Eksistē saistoši noteikumi attiecībā uz apstrādes nolūku, lai varētu ievērot nodalīšanas principu. Konkrētos nolūkos ievāktie dati tiek glabāti atsevišķi no citos nolūkos ievāktajiem datiem. Izmantotās IT sistēmas ļauj datus saglabāt atsevišķi (pateicoties iespējai izmantot vairākiem klientiem un piekļuves koncepcijām). Datu nodalīšana notiek testēšanas un produktīvajās sistēmās. Pseidonimizētu datu gadījumā reģistrētais atslēgas numurs, pēc kura atkal var identificēt personu, tiek saglabāts un uzglabāts atsevišķi. Pasūtījuma datu apstrādes vai funkciju pārnešanas laikā Izpildītājs dažādo Pasūtītāju datus apstrādā atsevišķi. Pateicoties esošo lomu un tiesību koncepciju veidam, ir iespējama apstrādāto datu loģiska nodalīšana.

4. Integritātes nodrošināšana

Lai nodrošinātu ievadīto datu protokolēšanu, ir ieviesti dažādi standarta pasākumi:

tiek protokolētas piekļuves tiesību izmaiņas un visas administratora darbības. Tiek protokolētas piekļuves ar rakstīšanas tiesībām (ievades, izmaiņas, dzēšana) un datu laukos veiktās izmaiņas (piem., no jauna ievadītā vai izmainītā datu ieraksta saturs). Tiek protokolētas pārsūtīšanas (piem, lejupielāde) un pieteikšanās darbības.

Izmantotie datu reģistrācijas dokumenti tiek dokumentēti un arhivēti, lai varētu izsekot ievadītajai informācijai. Protokolā tiek norādīts datums, laiks, lietotājs, darbības veids, lietojumprogramma un datu ieraksta kārtas numurs. Protokolēšanas iestatījumi tiek dokumentēti.

Protokolu datnēm var piekļūt tikai ar lasīšanas tiesībām. Personu loks, kam ir tiesības piekļūt protokolu datnēm, ir ļoti ierobežots (piem., tikai administrators, datu aizsardzības speciālists, revidents). Protokolu datnes tiek uzglabātas noteiktu laika periodu (piem., 1. gadu) un tad izdzēstas atbilstoši datu aizsardzības noteikumiem.

Protokolu datnes regulāri tiek automātiski izvērtētas. Protokolu datņu novērtējumi tiek sagatavoti pseidonimizētā formā, ja iespējams.

5. Pieejamības nodrošināšana

Arhitektūra ir veidota tā, ka iekšējie replicēšanas mehānismi AWS platformā jau pēc noklusējuma novērš datu zudumu. Lai nodrošinātu objekta aizsardzību, ir ieviesti šādi AWS standarta pasākumi:

tiek veikti ugunsdrošības pasākumi (piem., ugunsdrošas durvis, dūmu detektori, ugunsdrošības sienas, smēķēšanas aizliegums). Datoriekārtas ir pasargātas pret plūdiem (piem., datortelpa 1. stāvā, ūdens detektori). Tiek veikti pasākumi pret satricinājumiem (piem., datortelpa nav izvietota tālsatiksmes ceļu, sliežu, mašīntelpu tuvumā). Datoriekārtas ir nodrošinātas pret elektromagnētisko lauku iedarbību (piem., tērauda plates ārējās sienās). Tiek veikti pasākumi pret vandālismu un zādzībām (skat. informāciju par piekļuves kontroli). Datoriekārtas atrodas telpās ar atbilstošu klimatu (temperatūru un gaisa mitrumu regulē gaisa kondicionēšanas iekārta). Datoriekārtas ir aprīkotas ar pārsprieguma ierobežotājiem, lai novērstu pārspriegumu. Tiek veikti pasākumi, lai nodrošinātu netraucētu un nepārtrauktu elektroapgādi (piem UPS ierīces, ģeneratori).

Datubāzēm AWS platformā regulāri tiek veidotas dublējumkopijas. Dublējuma koncepcija ir dokumentēta un tā tiek regulāri pārbaudīta un atjaunināta. Dublēšanas datu nesēji ir pasargāti pret neatļautu piekļuvi. Izmantotās dublējuma programmas atbilst jaunākajiem kvalitātes standartiem un tiek regulāri atjauninātas. Ir ierīkots rezerves skaitļošanas centrs (tālu no apstrādes vietas), kur katastrofas gadījumā var turpināt datu apstrādi. Dažādie pieejamības kontroles pasākumi ir dokumentēti AWS Ārkārtas situāciju pārvarēšanas plānā.

Pirms tiek veikts datu apstrādes pasūtījumus, Izpildītājs tiek rūpīgi un pēc noteiktiem kritērijiem (tehniskie un organizatoriskie pasākumi) pārbaudīts. Tiek pieprasīts detalizēts apraksts par Izpildītāja veiktajiem tehniskajiem un organizatoriskajiem datu aizsardzības pasākumiem (atbildes uz uzdotajiem jautājumiem vai datu aizsardzības koncepcija) un šī informācija tiek pārbaudīta. Atkarībā no apstrādājamo datu apjoma un sensibilitātes pārbaude var tikt veikta arī uz vietas pie Izpildītāja. Izvēloties Izpildītājus, tiks ņemti vērā atbilstošie sertifikāti (piem., ISO 27001) Izpildītāja piemērotības noteikšanas process tiek atbilstoši un skaidri dokumentēts.

Lai nostiprinātu pasūtījuma saistības, starp Pasūtītāju un Izpildītāju tiek noslēgts pasūtījuma datu apstrādes līgums. Tajā ir detalizēti un rakstiski noteiktas abu Pušu kompetences un atbildības sfēras, kā arī pienākumi. Ja pilnvarotā pakalpojuma sniedzēja mītne atrodas ārpus ES vai EEZ, tiek piemērotas ES līguma standartklauzulas. Līgumā ir noteikts, ka Izpildītājs drīkst apstrādāt datus tikai saskaņā ar Pasūtītāja norādījumiem. Izpildītājam ir pienākums nekavējoties informēt Pasūtītāju, ja kāds no viņa dotajiem norādījumiem pēc Izpildītāja domām ir pretrunā datu aizsardzības noteikumiem. Lai tiktu ievērotas datu subjekta tiesības, pasūtījuma datu apstrādes līgumā tiek noteikts, ka Izpildītājam ir atbilstīgi jāatbalsta Pasūtītājs, piemēram, kad datu subjektiem ir jāsniedz piekļuve informācijai.

Turpmākās pasūtījuma datu apstrādes laikā Pasūtītājs formāli un saturiski kontrolē Izpildītāja darba rezultātus. Regulāri tiek pārbaudīts, vai Izpildītājs ievēro noteiktos tehniskos un organizatoriskos pasākumus. Galvenokārt ir jāuzrāda jaunākie atzinumi vai atbilstoši sertifikāti, respektīvi, dokumenti, kas pierāda, ka ir veikti IT drošības vai datu aizsardzības auditi. Ja tiek piesaistīti apakšuzņēmēji, līgumā ir notikts, ka tie ir atbilstoši jākontrolē.

6. Sistēmu noturības nodrošināšana

AWS mākoņa infrastruktūra ir izveidota kā elastīgākā un drošāka mākoņdatošanas vide. Tā ir izveidota visoptimālākajai pieejamībai, nodrošinot pilnīgu klientu nodalīšanu. Tā ir maksimāli mērogojama, darbības ziņā ļoti droša platforma, kas klientiem ļauj ātri un droši visā pasaulē piekļūt programmām un saturam. AWS pakalpojumi nav atkarīgi no satura, un visiem klientiem tiek nodrošināts vienādi augsts aizsardzības līmenis, neatkarīgi no satura veida vai ģeogrāfiskā reģiona, kur saturs ir saglabāts.

Pasaules līmeņa augstas drošības AWS skaitļošanas centri izmanto augstāko tehnoloģiju elektroniskās uzraudzības pasākumus un vairāku līmeņu piekļuves kontroles sistēmas. Skaitļošanas centros visu diennakti strādā apmācīti drošības speciālisti, turklāt piekļuve tiek atļauta tikai pēc mazu tiesību principa un tikai sistēmas administrācijas nolūkos.

7. Personas datu pieejamības atjaunošanas process gadījumā, ja ir noticis fizisks vai tehnisks negadījums

AWS skaitļošanas centri tiek ierīkoti klasteros dažādos pasaules reģionos. Visi skaitļošanas centri ir tiešsaistē un apkalpo klientus; neviens no centriem nav atslēgts. Atteices gadījumā automatizētie procesi novirza klientu datu plūsmu prom no skartās zonas. Galvenās programmas ir sagatavotas N+1 konfigurācijā, kas nozīmē to, ka skaitļošanas centra atteices gadījumā ir pieejama pietiekama kapacitāte, lai datu plūsmu pa apjomiem sadalītu pa atlikušajiem centriem.

AWS piedāvā elastību, novietošanas instances un iespēju saglabāt datus vairākos ģeogrāfiskajos reģionos un vairākās pieejamības zonās atsevišķos reģionos. Katra pieejamības zona ir izstrādāta kā neatkarīga atteices zona. Tas nozīmē, ka pieejamības zonas fiziski ir izvietotas tipiskā pilsētas rajonā un atrodas, piem., apgabalos, kur ir mazs plūdu risks (atkarībā no reģiona ir dažādas plūdu zonu kategorijas). Papildus patstāvīgajai nepārtrauktajai barošanai un ģeneratoriem, kas atrodas uz vietas centrā, pieejamības zonas ar elektrību apgādā neatkarīgas elektroapgādes stacijas, lai minimizētu atsevišķu kļūdu vietas. Visas pieejamības zonas ir savienotas arī ar vairākiem Tier 1 Transit nodrošinātājiem.

Negadījumu pārvaldīšanai Amazon komanda izmanto jomā ierastās diagnostikas metodes, lai paātrinātu būtisku uzņēmuma darbību traucējošu negadījumu novēršanu. Uzņēmuma personāls ir pieejams visu diennakti, septiņas dienas nedēļā un 365 dienas gadā, lai konstatētu traucējumus un to sekas un novērstu šos traucējumus.

8. Tehnisko un organizatorisko pasākumu regulāro efektivitātes pārbaužu, novērtēšanas un izvērtēšanas process

Uzņēmumā pieejamās vadlīnijas un norādījumi, respektīvi, ieviestie informācijas drošības standarti, tiek piemēroti arī RIO platformas ieviešanā un darbībā. Uzņēmumā ir amati datu aizsardzības un informācijas drošības jomā (datu aizsardzības speciālists un informācijas drošības speciālists) Visiem nodarbinātajiem ir jāievēro datu konfidencialitāte un tie ar brošūru, informatīvo izdevumu, iekštīkla norādījumu palīdzību ir informēti par datu drošību un IT drošības pasākumiem.

Interneta procesi attiecībā uz datu aizsardzības tehnisko un organizatorisko pasākumu ievērošanu tiek pārbaudīti revīzijas laikā, informācijas drošības un datu aizsardzības pārbaužu laikā.

Apstrādes procesi un datu aizsardzības pasākumi tiek dokumentēti apstrādes darbību katalogā. Regulāri tiek veiktas pārbaudes (iekšējās un ārējās), lai pārbaudīti pasākumu efektivitāti.