LOGISTIK IM FLUSS.

Acord privind prelucrarea datelor cu caracter personal (conform art. 28 RGPD)

Încheiat între

utilizator (așa cum este acesta definit în contractul principal)

(denumit în continuare „**contractant**”)

și

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

(denumit în continuare „**beneficiar**”)
(în continuare, beneficiarul și contractantul vor fi desemnați prin termenul de „**parte contractuală**”, iar atunci când se face referire la ambii, aceștia vor fi desemnați prin termenul de „**părți contractuale**”).

Preambul

(A) Prezentul acord privind prelucrarea datelor cu caracter personal (denumit în continuare „**contract**”) se aplică pentru toate activitățile în cadrul cărora contractantul are acces la date cu caracter personal (așa cum sunt acestea definite la pct. 1.5 de mai jos) care fac referire la beneficiar, furnizori terți sau oricare alte persoane în contextul desfășurării activității descrise la pct. 2 din Termenii și condițiile generale privind utilizarea Platformei și, eventual, în cadrul contractelor individuale încheiate pentru prestarea altor servicii (denumite în continuare „**contract principal**”)**.**

(B) În cadrul acestui contract, beneficiarul acționează în calitate de operator de date cu caracter personal iar contractantul, în calitate de persoană împuternicită pentru prelucrarea datelor cu caracter personal, în conformitate cu art. 28 RGPD.

Prin urmare, părțile contractuale convin următoarele:

1 Definiții și interpretare

1.1 Termenul de „**legislație europeană**” desemnează legislația aplicabilă a Uniunii Europene, legile aplicabile ale statelor membre actuale ale Uniunii Europene, precum și legile aplicabile ale oricărui stat care devine ulterior stat membru al Uniunii Europene.

1.2 Termenul de „**legislație europeană privind protecția datelor cu caracter personal**” desemnează legislația aplicabilă a Uniunii Europene referitoare la prelucrarea datelor cu caracter personal (în special, RGPD), legile aplicabile ale statelor membre actuale ale Uniunii Europene privind prelucrarea datelor cu caracter personal (în special, regulamentul BDSG, în versiunea aflată în vigoare), precum și legile aplicabile pentru prelucrarea datelor cu caracter personal ale fiecărui stat care devine ulterior devine stat membru al Uniunii Europene.

1.3 Acronimul „**RGPD**” face referire la „REGULAMENTUL (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI din data de 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)”.

1.4 Acronimul „**BDSG**” face referire la Legea federală germană privind protecţia datelor.

1.5 Termenul de „**date cu caracter personal**” este utilizat aici conform definiţiei date acestui termen în BDSG/RGPD.

2 Obiectul prelucrării datelor cu caracter personal/obligaţiile beneficiarului

2.1 Acest contract reglementează obligaţiile părţilor contractuale în ceea ce privește prelucrarea de către contractant a datelor cu caracter personal care aparţin beneficiarului în cadrul executării contractului principal menţionat în Anexa 1.

2.2 Obiectul, durata, natura şi scopul prelucrării datelor cu caracter personal, tipul datelor cu caracter personal, categoriile de persoane vizate, precum şi obligaţiile şi drepturile operatorului de date cu caracter personal sunt stipulate în Anexa 1 a prezentului contract şi în caietul de sarcini aferent contractului principal.

2.3 Beneficiarul rămâne operator de date cu caracter personal în conformitate cu RGPD şi garantează admisibilitatea prelucrării datelor cu caracter personal ale persoanelor vizate (şoferi şi eventual alte persoane). În acest context, beneficiarul îşi îndeplineşte, în special, pe deplin obligaţia de informare şi se asigură că există un temei legal corespunzător pentru prelucrarea datelor cu caracter personal (de exemplu, încheierea unui acord la nivel de întreprindere, limitarea prelucrării la scopuri ce ţin de raportul de muncă).

3 Obligaţiile contractantului

3.1 Contractantul prelucrează datele cu caracter personal aparţinând beneficiarului exclusiv în scopurile menţionate în Anexa 1 şi cu respectarea prevederilor contractului principal, precum şi în numele şi în conformitate cu instrucţiunile beneficiarului, prezentate în Anexa 1; contractantul nu va procesa datele cu caracter personal care fac obiectul prezentului contract în niciun alt scop. Această prevedere nu se aplică pentru prelucrarea în scopuri proprii a datelor care nu fac obiectul prezentului contract, în conformitate cu prevederile de la pct. 8.3.4 din contractul principal. Nu vor fi create niciun fel de copii sau duplicate ale datelor cu caracter personal fără ca beneficiarul să aibă cunoştinţă de cauză cu privire la acest lucru. Această prevedere nu include copiile de rezervă, în măsura în care acestea sunt necesare pentru a asigura o prelucrare adecvată a datelor şi nici datele care trebuie să fie păstrate în temeiul cerinţelor legale aplicabile privind păstrarea documentelor.

3.2 După încetarea furnizării serviciilor de prelucrare de date, contractantul trebuie, în funcţie de dorinţa exprimată de beneficiar, să îi predea beneficiarului toate datele cu caracter personal care îi aparţin acestuia, şi/sau să şteargă datele respective, cu respectarea clauzelor de confidenţialitate, în măsura în care acest lucru nu se află în contradicţie cu perioadele de păstrare legale şi în cazul în care contractantul nu urmează să prelucreze aceste date în scopuri proprii care nu fac obiectul prezentului contract, în conformitate cu prevederile de la pct. 8.3.4 din contractul principal. Această prevedere se aplică şi pentru materialele utilizate la realizarea de teste şi rebuturi. Ştergerea, respectiv predarea completă a datelor către beneficiar se va realiza la cererea acestuia, împreună cu menţionarea datei şi confirmarea scrisă.

3.3 Atâta timp cât acest lucru este inclus în descrierea serviciilor, contractantul îl asistă pe beneficiar la exercitarea drepturilor persoanei vizate (dreptul la informare, dreptul la rectificare, dreptul de opoziţie, dreptul la ştergerea datelor) conform îndrumărilor primite în acest sens de la beneficiar.

3.4 Contractantul confirmă, în măsura în care acest lucru este impus de lege, faptul că a solicitat serviciile unui responsabil cu protecţia datelor cu caracter personal (a se vedea art. 38 BDSG şi art. 37 RGPD).

3.5 Contractantul se obligă să notifice imediat beneficiarul cu privire la rezultatele verificărilor efectuate de autorităţile însărcinate cu monitorizarea protecţiei datelor cu caracter personal, în măsura în care verificările respective au legătură cu prelucrarea datelor cu caracter personal care aparţin beneficiarului. Contractantul va remedia în termen util eventualele deficienţe semnalate şi va informa beneficiarul cu privire la acest lucru.

3.6 Prelucrarea datelor realizată de către contractant şi de către subcontractanţii autorizaţi de beneficiar are loc exclusiv pe teritoriul Republicii Federale Germania, într-un stat membru al Uniunii Europene sau într-un alt stat semnatar al Acordului privind Spaţiul Economic European. Un eventual transfer către o altă ţară (denumită în continuare „**ţară terţă**”) necesită acordul expres al beneficiarului, formulat în prealabil, şi poate avea loc numai dacă sunt îndeplinite condiţiile speciale care privesc exportul de date către ţări terţe (a se vedea art. 40 şi următoarele RGPD). Pentru aceasta, în Anexa 1 trebuie să fie făcute menţiunile necesare, şi, dacă este cazul, să fie anexate documentele (contractuale) suplimentare.

3.7 Contractantul are obligaţia de a-i familiariza pe angajaţii săi însărcinaţi cu realizarea lucrărilor cu dispoziţiile aplicabile referitoare la protecţia datelor cu caracter personal şi să obţină angajamentul acestora cu privire la respectarea caracterului confidenţial al datelor respective (a se vedea art. 28 RGPD, alin. 3 b), precum şi să se asigure, prin măsuri corespunzătoare, că aceşti angajaţi prelucrează date cu caracter personal numai la indicaţia beneficiarului.

3.8 Contractantul monitorizează în mod regulat respectarea prevederilor referitoare la protecţia datelor menţionate în acest contract şi în cadrul instrucţiunilor documentate aparţinând beneficiarului pe întreaga durată a contractului. Rezultatele verificărilor vor fi prezentate beneficiarului la cererea

acestuia, în măsura în care acestea sunt relevante pentru prelucrarea datelor care aparţin beneficiarului. Măsurile de monitorizare sunt descrise în cadrul unui concept de protecţie a datelor care trebuie să fie prezentat beneficiarului la cererea acestuia.

3.9 Contractantul trebuie să ofere beneficiarului sprijinul necesar pentru respectivul tip de prelucrare a datelor şi, dacă acest lucru este posibil, asistenţa tehnică şi organizatorică necesară pentru ca acesta să îşi poată îndeplini obligaţia de a răspunde solicitărilor în legătură cu drepturile menţionate în capitolul III RGPD care le revin persoanelor vizate. Beneficiarul va suporta costurile rezultate în partea contractantului ca urmare a acestui lucru.

3.10 Contractantul trebuie să ofere beneficiarului sprijinul necesar pentru respectivul tip de prelucrare a datelor şi să-i pună acestuia la dispoziţie toate informaţiile de care dispune în vederea îndeplinirii obligaţiilor prevăzute de art. 32-36 din RGPD.

4 Măsuri tehnice şi organizatorice privind securitatea datelor

4.1 Contractantul va lua măsuri tehnice şi organizatorice adecvate pentru asigurarea protecţiei datelor (a se vedea art. 32 RGPD). Contractantul are, în special, obligaţia de a pune în aplicare toate măsurile tehnice şi organizatorice menţionate în Anexa 2 a acestui contract. În cursul derulării contractului, aceste măsuri trebuie să fie adaptate de către contractant la nivelul curent de dezvoltare tehnică şi organizaţională, fără ca acest lucru să implice o reducere a nivelului de protecţie. Toate modificările majore trebuie să fie convenite în scris.

4.2 Contractantul va informa beneficiarul la cererea acestuia cu privire la respectarea efectivă a măsurilor tehnice şi organizatorice.

4.3 Contractantul are obligaţia a pune la dispoziţie o documentaţie adecvată pentru prelucrarea datelor, pe baza căreia beneficiarul să poată face dovada prelucrării corecte a datelor. Documentele doveditoare pot, de asemenea, să fie furnizate printr-o procedură de certificare aprobată în conformitate cu art. 42 RGPD.

5 Subcontractanţi

5.1 Contractantul este autorizat să angajeze subcontractanţii enumeraţi în Anexa 1.

5.2 Prin prezenta, se aprobă posibilitatea de angajare a altor subcontractanţi. Cu toate acestea, contractantul are obligaţia de a informa beneficiarul cu privire la orice modificare pe care acesta intenţionează să o întreprindă în legătură cu implicarea sau înlocuirea subcontractanţilor; beneficiarul ridica obiecţii cu privire la modificările pe care contractantul intenţionează să le întreprindă. Serviciile realizate de terţi pe care contractantul le utilizează ca servicii auxiliare care să asigure executarea contractului nu fac obiectul prevederii de mai sus referitoare la subcontactanţi. Acestea includ, de

exemplu, servicii de telecomunicații, personal de curățare, auditori sau eliminarea ca deșeuri a suporturilor de date. Cu toate acestea, contractantul are obligația de a încheia acorduri contractuale adecvate și conforme cu dispozițiile legale aplicabile și să ia măsurile necesare de control pentru a asigura protecția și securitatea datelor care aparțin beneficiarului, chiar și pentru serviciile externalizate.

5.3 În cazul în care contractantul apelează la serviciile unui subcontractant, contractantul trebuie să se asigure că acesta face obiectul aceloraşi obligații privind protecția datelor aplicabile în temeiul (i) unui contract care urmează să fie încheiat între subcontractant și contractant sau (ii) altor instrumente juridice ale legislației europene privind protecția datelor. În special, contractantul trebuie să se asigure că subcontractantul oferă garanții rezonabile cu privire la faptul că vor fi întreprinse măsurile tehnice și organizaționale corespunzătoare astfel încât prelucrarea datelor cu caracter personal să fie realizată în conformitate cu cerințele BDSG/RGPD. La cererea scrisă din partea beneficiarului, contractantul va furniza beneficiarului informații privind conținutul esențial al contractului și îndeplinirea obligațiilor privind protecția datelor în cadrul relațiilor subcontractuale, dacă este necesar, prin prezentarea documentelor contractuale relevante. Referitor la acestea, contractantul este îndeptățit să facă ilizibile informațiile referitoare la condițiile comerciale. Clientul este obligat să respecte caracterul confidențial al informațiilor obținute pe această cale.

6 Dreptul privind efectuarea de controale

6.1 Beneficiarul are dreptul de controla ele însuși sau prin intermediul unor terți desemnați de acesta îndeplinirea obligațiile care decurg din prezentul contract (inclusiv a instrucțiunilor emise).

6.2 Contractantul va oferi beneficiarului sprijinul necesar pe toată durata efectuării controalelor. În special, contractantul va acorda acces la echipamentele de prelucrare a datelor și va furniza toate informațiile necesare.

6.3 În cazul în care o anumită verificare are drept rezultat faptul că contractantul nu a respectat termenii prezentului contract și/sau termenii Legii Europene privind Protecția Datelor, contractantul va lua toate măsurile corective necesare pentru a se conforma condițiilor stipulate în baza acestui contract și/sau Legislației Europene privind Protecția Datelor.

6.4 Beneficiarul va suporta toate costurile rezultate în partea acestuia ca urmare a exercitării dreptului de control. Cu privire la costurile rezultate în partea contractantului ca urmare a efectuarii unei operații de control realizate de către beneficiar, contractantul are posibilitatea de a solicita beneficiarului acoperirea acestor costuri, în cazul în care beneficiarul efectuează singur sau prin intermediul unor terți mai mult de o verificare în decursul unui an calendaristic.

6.5 Verificările efectuate la sediul contractantului trebuie să fie anunțate în timp util și să nu afecteze în mod disproporționat operațiunile comerciale ale contractantului.

7 Obligațiile de notificare

Contractantul va informa imediat beneficiarul în cazul în care acesta consideră că o anumită instrucțiune primită din partea beneficiarului încalcă Legislația europeană privind protecția datelor cu caracter personal. Instrucțiunea cu privire la care se dovedește că obiecțiile ridicate sunt întemeiate va fi urmată numai în cazul în care aceasta este modificată sau confirmată explicit de către beneficiar. Contractantul nu este obligat să revizuiască instrucțiunile din punct de vedere material sau juridic.

Contractantul va informa imediat beneficiarul în cazul detectării unor erori sau unor nereguli cu privire la prelucrarea datelor sau în cazul unei încălcări presupuse a prevederilor privind protecției datelor (denumite în continuare în mod colectiv, prin termenul de „**incident**"). Beneficiarul trebuie să documenteze incidentul împreună cu toate circumstanțele și efectele aferente acestuia, respectiv să documenteze toate măsurile de remediere întreprinse, iar la cererea beneficiarului aceste informații documentate vor fi trimise beneficiarului, în scris sau în format electronic.

8 Răspundere și aprobare

8.1 Contractantul este răspunzător pentru prejudiciile cauzate de intenția și/sau neglijența gravă acestuia sau agenților care acționează în numele său. Pentru daunele datorate simplei neglijențe a contractantului sau agenților care acționează în numele acestuia, contractantul va răspunde numai în cazul în care este încălcată o obligație cardinală. Obligațiile cardinale reprezintă obligații contractuale esențiale care fac posibilă executarea corespunzătoare a contractului și cu privire la care beneficiarul trebuie să fie asigurat de respectarea acestora. În cazul unei simple neglijențe privind încălcarea unor astfel de obligații cardinale, răspunderea contractantului se limitează la daunele tipice previzibile.

8.2 Beneficiarul exonerează contractantul de toate pretențiile venite din partea terților (inclusiv din partea persoanele afectate și/sau autorităților însărcinate cu protecția datelor), de daunele și cheltuielile rezultate ca urmare a încălcării de către beneficiar a prevederilor prezentului contract și/sau Legislației europene privind protecția datelor cu caracter personal; acest lucru nu se aplică în cazul în care beneficiarul nu se face vinovat de încălcarea respectivelor prevederi sau dacă contractantul a contribuit la încălcarea acestora.

9 Durată

Durata acestui contract corespunde duratei contractului principal. Odată cu încetarea contractului principal, indiferent de temeiul în baza căreia se realizează acest lucru, are loc și rezilierea automată a acestui contract. Această prevedere nu aduce atingere clauzei privind încetarea contractului în baza unui temei obiectiv.

10 Alte menţiuni

10.1 Serviciile prestate de contractant în temeiul prezentului contract vor fi achitate pe baza sistemului de remunerare stabilit în cadrul contractului principal.

10.2 În cazul în care datele cu caracter personal ale beneficiarului aflate la contractant sunt puse în pericol ca urmare a unor măsuri întreprinse de terţi (ca de exemplu, sechestru sau confiscare), a unor proceduri de faliment sau de compensare sau a altor evenimente similare, contractantul are obligaţia de a informa imediat beneficiarul cu privire la acest lucru.

10.3 În cazul în care anumite prevederi ale prezentului contract sunt sau devin nule din punct de vedere juridic, acest lucru nu va afecta valabilitatea celorlalte prevederi. În cazul în care o anumită cauză devine nulă, părţile contractuale vor conveni o altă reglementare substitutivă bazată pe aspectele obiective şi economice ale contractului.

10.4 În cazul în care Marea Britanie se retrage din Uniunea Europeană, contractantul se angajează să finalizeze toate acordurile încheiate şi să întreprindă toate măsurile necesare pentru ca prelucrarea datelor pe teritoriul Marii Britanii în baza contractului încheiat să fie permisă din punct de vedere juridic de la data retragerii acesteia din Uniunea Europeană. În măsura în care nu există o decizie de adecvare pozitivă a Comisiei Europene la momentul retragerii din Uniunea Europeană, clauzele aplicabile sunt reprezentate, în special, de clauzele standard privind protecţia datelor în conformitate cu articolul 46 paragraful (2) litera (c) pentru transferul de date cu caracter personal către operatorii de date stabiliţi în ţări terţe în care nu se asigură un nivel adecvat de protecţie.

În cazul în care contractantul nu îndeplineşte aceste obligaţii, beneficiarul este îndreptăţit să solicite contractantului, cu efect de la retragerea Marii Britanii din Uniunea Europeană, ca serviciile respective să fie furnizate de o societate afiliată, respectiv de o societate cu sediul permanent pe teritoriul Uniunii Europene, fără ca acest lucru să implice pentru beneficiar un efort financiar mai mare sau costuri suplimentare.

10.5 Acest acord privind prelucrarea datelor cu caracter personal este disponibil în 18 limbi, cu observaţia că versiunea originală în limba germană este prioritară în cazul eventualelor neconcordanţe.

10.6 Acest contract se supune legii Republicii Federale Germania, cu excluderea Convenţiei Naţiunilor Unite asupra contractelor de vânzare. Sediul procedural unic se află în München.

10.7 Următoarele anexe reprezintă parte integrantă a contractului:

Anexa 1 – Descrierea prelucrării datelor cu caracter personal
Anexa 2 – Măsuri tehnice şi organizatorice

ANEXA 1 – Descrierea prelucrării datelor cu caracter personal

1 Contract principal

Contractul principal, așa cum este acesta definit la pct. 2.1 al părții principale a contractului, este reprezentat de „Termenii și condițiile generale privind utilizarea Platformei".

Titlu/părți contractuale: **TB Digital Services GmbH**, cu sediul în Oskar-Schlemmer-Str. 19 - 21, 80807 München / **utilizatorul**

2 Obiectul și durata contractului

Obiectul contractului rezultă pe baza precizărilor de la pct. 1 (*Obiectul*) și pct. 8 (*Datele utilizatorului și protecția datelor*) din contractul principal; durata contractului este specificată la pct. 7 (*Încheierea contractului, durata contractului și drepturile privind rezilierea*) din contractul principal.

3 Domeniul de aplicare, tipul și scopul prelucrării datelor cu caracter personal/măsurilor de prelucrare a datelor cu caracter personal

Domeniul de aplicare, tipul și scopul prelucrării datelor cu caracter personal sunt specificate la pct. 8 al contractului principal.

Descrierea detaliată a obiectului contractului în ceea ce privește domeniul de aplicare, tipul și scopul:

Pentru a putea furniza serviciile oferite de contractant (așa cum sunt acestea definite în contractul principal), contractantul trebuie să transfere datele cu caracter personal aparținând beneficiarului prin intermediul aplicațiilor Connected Vehicles sau Mobile Devices (și eventual, datele cu caracter personal transferate aparținând unui furnizor terț cu care utilizatorul a convenit furnizarea unor servicii terțe) pentru furnizarea serviciilor convenite și pentru transmiterea către și salvarea acestora pe platforma contractantului. Contractantul va procesa datele stocate pe platformă în măsura în care acest lucru este necesar pentru furnizarea serviciilor contractate (de exemplu, pentru a analiza și evalua comportamentul rutier al șoferului, precum și pentru utilizarea aplicațiilor Connected Vehicle sau Mobile Device pe baza datelor cu caracter personal și pentru a putea pune la dispoziție beneficiarului pe baza acestora oferte personalizate, așa cum sunt instruirea șoferilor, detalii despre echipamente, precum și recomandări pentru creșterea eficienței). Domeniul exact de aplicare, tipul și scopul sunt definite, în special, pe baza contractelor individuale suplimentare care urmează să fie încheiate.

4 Persoanele care fac obiectul contractul încheiat (categorii de persoane vizate)

Persoanele vizate de prelucrarea datelor cu caracter personal sunt următoarele grupuri de persoane:

- **Şoferi şi alţi angajaţi** (angajaţii companiei ce aparţine beneficiarului), de exemplu, salariaţi, practicanţi, candidaţi, foşti angajaţi*;*
- **Şoferi**, care nu sunt angajaţi ai companiei;
- **Persoanele de contact** ale companiilor de încărcare/descărcare marfă sau ai altor parteneri de afaceri ai beneficiarului; şi
- **Angajaţii Grupului** (angajaţii unei alte companii aparţinând Grupului beneficiarului).

5 Tipul datelor cu caracter personal

Prelucrarea datelor cu caracter personal include următoarele tipuri de date cu caracter personal:

- Numele şoferului şi numărul de identificare a şoferului;
- Numărul de identificare a vehiculului;
- Datele de localizare;
- Date referitoare la timpii de conducere şi de odihnă;
- Date referitoare la comportamentul rutier;
- Datele de stare ale Connected Vehicle;
- Datele de stare ale remorcii;
- Datele de stare ale suprastructurilor şi elementelor ataşabile, agregatelor şi altor componente ale vehiculului;
- Datele de stare ale eventualelor dispozitive IOT conectate
- Datele de stare ale Mobile Devices;
- Datele referitoare la încărcătură;
- Datele referitoare la comanda de lucru; şi
- Datele de contact ale persoanelor de contact din partea companiilor de încărcare/descărcare marfă sau altor parteneri de afaceri ai beneficiarului.

6 Instrucţiuni documentate

Beneficiarul instruieşte contractantul să preilucreze datele cu caracter personal conform pct. 8 din contractul principal. Aceasta include, în special, următorul tip de prelucrare date:

- Datele cu caracter personal sunt transmise prin intermediul aplicaţiilor Connected Vehicle sau Mobile Device către şi salvate pe platforma bazată pe tehnologia cloud a contractantului.
- Datele cu caracter personal sunt prelucrate în baza prezentului contract numai dacă acestea sunt necesare pentru îndeplinirea contractului principal; Această prevedere nu aduce atingere clauzei specificate la pct. 8.3.4 al contractului principal.

- Contractantul transmite datele cu caracter personal unui furnizor terţ (aşa cum acesta este definit în contractul principal) dacă şi în măsura în care acest transfer către furnizorul terţ este necesar pentru a putea furniza beneficiarului serviciile sale terţe (aşa cum sunt acestea definite în contractul principal).
- Contractantul va analiza şi evalua comportamentul rutier al şoferului, precum şi utilizarea aplicaţiei Connected Vehicle pe baza datelor cu caracter personal şi pentru a putea pune la dispoziţie beneficiarului pe baza acestora oferte personalizate, aşa cum sunt instruirea şoferilor, detalii despre echipamente, precum şi recomandări pentru creşterea eficienţei.

7 Locul unde are loc prelucrarea datelor

- Germania.
- Regatul Unit; în cazul în care datele sunt prelucrate în cadrul Uniunii Europene pentru servicii de hosting IT şi/sau suport IT, trebuie să fie încheiate contracte adecvate privind prelucrarea datelor cu caracter personal.
- În cazul în care contractantul apelează la subcontractanţi din afara Uniunii Europene pentru servicii de hosting IT şi/sau suport IT (a se vedea pct. 8 din prezenta Anexă 1), transferul de date cu caracter personal va avea loc pe baza unor clauze contractuale standard/clauze de protecţie a datelor standard pentru transferul de date cu caracter personal către persoane împuternicite pentru prelucrarea acestor date din ţări terţe, încheiate între contractant şi subcontractant, conform art. 46 alin. 2 c) RGPD.

8 Subcontractanţi

Contractantul va apela la serviciile furnizate de următorii subcontractanţi (care pot, la rândul lor, să apeleze la serviciile furnizate de alţi subcontractanţi):

Nr.	Subcontractant (companie, adresă, persoană de contact)	Categorii de date prelucrate	Etapele/scopul prelucrării datelor realizate de subcontractanți
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Toate datele cu caracter personal de pe platformă care au legătură cu activitatea de vânzare (altfel spus, locația unde un anumit client se poate înregistra pe platformă și poate plasa comenzi)	Platforma de hosting
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Toate datele cu caracter personal de pe platformă care au legătură cu activitatea de vânzare (altfel spus, locația unde un anumit client se poate înregistra pe platformă și poate plasa comenzi)	Suportul IT privind platforma
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 SUA https://aws.amazon.com/de/compliance/contact/	Toate celelalte date de utilizator cu caracter personal transmise contractantului prin intermediul vehiculului	Platforma de hosting/suportul IT privind platforma
4	Eventual, în viitor, acest item va înlocui nr. 3: Amazon Webservices (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 SUA https://aws.amazon.com/de/compliance/contact/	Toate celelalte date de utilizator cu caracter personal transmise contractantului prin intermediul vehiculului	Platforma de hosting
5	MAN Service und Support GmbH Dachauer Straße 667	Toate datele cu caracter personal necesare pentru procesarea întrebărilor clienților în timpul	Asistență tehnică de nivel 1

	80995 München Germania	asistenței tehnice de nivel 1 și nivel 2	
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 SUA	Toate datele cu caracter personal necesare procesării facturării/procesării comenzilor	Platforma de hosting (EU Tenant – Gehosted by Amazon Web Services (EU) – a se vedea pct. 4
7	MAN Truck & Bus AG Dachauer Str. 667 80995 München Germania	Toate celelalte date de utilizator cu caracter personal transmise contractantului prin intermediul aplicațiilor Connected Vehicle și/sau Mobile Device	Platforma de hosting
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Germania	Toate celelalte date de utilizator cu caracter personal transmise contractantului prin intermediul vehiculelor dotate cu TBM1/2	Platforma de hosting
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Suedia	Toate celelalte date de utilizator cu caracter personal transmise contractantului prin intermediul vehiculului	Platforma de hosting
10	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hannover Germania	Toate celelalte date de utilizator cu caracter personal transmise contractantului prin intermediul vehiculului	Platforma de hosting

ANEXA 2 – Măsuri tehnice şi organizatorice

Măsurile tehnice şi organizatorice care trebuie să fie întreprinse de contractant pentru a asigura un nivel de protecţie corespunzător riscului existent sunt descrise în cadrul conceptului privind protecţia datelor aferent platformei RIO, iar acestea includ, în special:

1. Pseudonimizare

Atâta timp cât datele cu caracter personal sunt utilizate în scopuri de evaluare care pot fi, de asemenea, realizate cu ajutorul unor date pseudonime, se vor utiliza tehnici de pseudonimizare. În acest caz, se va stabili în prealabil pentru fiecare câmp de date dacă acesta trebuie să fie pseudonimizat deoarece, în caz contrar, acesta ar permite identificarea persoanei reale căreia aparţin datele respective. Cheile de pseudonimizare vor fi stocate într-un director „Data Safe" pentru care va setată o restricţie maximă privind accesul.

2. Criptare

Dispozitivele mobile comunică în mod criptat cu terminalul de recepţie folosind un certificat de dispozitiv individual. Datele vor fi transmise în cadrul platformei RIO în formă criptată („Ubiquitous encryption" sau „encryption everywhere").

3. Asigurarea confidenţialităţii

Toţi angajaţii sunt şi vor fi instruiţi cu privire la obligaţiile care le revin privind asigurarea confidenţialităţii datelor, iar aceştia se vor angaja în scris să păstreze confidenţialitatea datelor.

Infrastructura IT utilizată este furnizată de Amazon Web Services (denumită în continuare AWS) ca parte a tehnologiei cloud (IaaS & PaaS). Controlul accesului va fi asigurat de operatorul Centrului de Date AWS: Centrele de Date AWS extrem de sigure utilizează sisteme de supraveghere electronică de ultimă generaţie şi sisteme de control al accesului pe mai multe niveluri. Centrele de Date dispun în permanenţă de personal de securitate instruit, iar accesul este acordat strict în conformitate cu principiul privind acordarea a cât mai puţine drepturi şi doar în scopul asigurării administrării sistemului.

Accesul la componentele hardware (Clients) ale TB Digital Services GmbH are loc cu ajutorul unor măsuri standard optime, aplicabile pentru fiecare caz în parte. Acestea sunt reprezentate, de exemplu, de restricţii de acces realizate pe baza unor sisteme de separare (turnichete), sisteme de supraveghere video, sisteme de alarmă şi/sau securitate, uşi securizate electronic sau mecanic, clădiri antifurt, autorizaţii de acces documentate (vizitatori, personal extern) sau zone de securitate declarate.

Controalele de acces includ măsuri pentru securitatea dispozitivelor, securitatea reţelei şi securitatea aplicaţiilor.

Vor fi luate mai multe măsuri diferite pentru asigurarea siguranţei dispozitivelor montate pe vehicul: Dispozitivele mobile sunt instalate permanent pe vehicul şi dispun de Secure Boot, altfel spus, nu este posibilă

încărcarea şi lansarea unui alt sistem de operare. Dispozitivele mobile comunică în mod criptat cu terminalul de recepţie folosind un certificat de dispozitiv individual. Datele vor fi transmise în cadrul platformei RIO în formă criptată („Ubiquitous encryption" sau „encryption everywhere"). Dispozitivele de recepţie sunt menţinute în permanenţă la standardele actuale de securitate prin intermediul instalării regulate a actualizărilor de securitate (managementul patch-urilor).

Pentru asigurarea siguranţei reţelei vor fi luate, de asemenea, mai multe măsuri standard: Este necesar să implementate specificaţiile corecte (conform standardelor tehnice actuale) ale parolei (lungime parolă, complexitate, perioada de valabilitate etc.). Introducerea incorectă, în mod repetat, a combinaţiei ID utilizator/parolă duce la blocarea (temporară) a ID-ului utilizatorului. Reţeaua de întreprinderi este protejată cu ajutorul unei aplicaţii firewall în faţa reţelelor deschise nesigure. A fost creat un proces care asigură alimentarea regulată a dispozitivelor mobile cu actualizări de securitate (proces OTA). Pentru a detecta, respectiv pentru a evita eventualele atacuri asupra reţelei de întreprinderi (Intranet) vor fi utilizate tehnologii adecvate (ca de exemplu, Intrusion Detection Systeme). Angajaţii vor fi informaţi în mod regulat cu privire la pericolele şi riscurile existente.

Pentru asigurarea siguranţei aplicaţiilor vor fi luate, de asemenea, mai multe măsuri standard:

Aplicaţiile relevante vor fi protejate împotriva accesului neautorizat cu ajutorul mecanisme adecvate de autentificare şi autorizare. Este necesar să implementate specificaţiile corecte (conform standardelor tehnice actuale) ale parolei (lungime parolă, complexitate, perioada de valabilitate etc.). În cazul aplicaţiilor care necesită măsuri speciale de protecţie vor fi utilizate mecanisme puternice de autentificare (de exemplu,Token, PKI). Introducerea incorectă, în mod repetat, a combinaţiei ID utilizator/parolă duce la blocarea (temporară) a ID-ului utilizatorului. Datele utilizate în cadrul proceselor relevante vor fi stocate în formă criptată pe un suport de date mobil. Vor fi înregistrate toate accesările şi încercările de accesare a aplicaţiilor. Fişierele de logare generate vor fi păstrate pentru o perioadă adecvată de timp (cel puţin 90 de zile) şi vor fi verificate (aleatoriu).

Autorizările utilizatorilor (privind accesul şi utilizarea) vor fi asigurate prin intermediul mai multor măsuri diferite, iar acestea vor fi atribuite întotdeauna unei singure persoane. Alocarea autorizărilor reprezintă responsabilitatea managerului platformei, iar aceasta va fi revizuită în mod regulat. Acordarea autorizaţiilor de acces va avea loc doar pe baza unui proces bine definit şi documentat. Modificările aduse autorizaţiilor de acces vor fi realizate pe baza principiului verificării efectuate de două persoane, iar acestea vor fi documentate în cadrul unui fişier de logare.

Pentru asigurarea verificării şi controlului accesului vor fi luate mai multe măsuri diferite: Drepturile de acces sunt definite şi documentate ca parte a unui concept de rol/autorizare şi sunt atribuite rolurilor respective în funcţie de cerinţele aplicabile pentru sarcinile de lucru. Vor fi stabilite roluri/autorizări specifice pentru administratorii tehnici (care, dacă acest lucru este posibil din punct de vedere tehnic, nu permit accesul la date cu caracter personal). Vor fi stabilite roluri/autorizări specifice pentru personalul de asistenţă tehnică (care nu includ drepturi de administrare tehnică).

Specificarea rolurilor/autorizărilor şi atribuirea rolurilor/autorizărilor, dacă acest este posibil din punct de vedere tehnic şi organizaţional, nu trebuie să fie realizate de aceleaşi persoane şi în cadrul aceleiaşi proceduri de verificare (aprobare), iar acestea trebuie să fie valabile pentru o perioadă limitată de timp. Accesarea directă a bazei de date, ocolind conceptul de rol/autorizare, va fi posibilă numai pentru administratorii autorizaţi ai bazelor de date. Există un regulament privind utilizarea suporturilor private de date, respectiv este interzisă utilizarea suporturilor private de date. Există reglementări obligatorii privind accesarea datelor în cazul întreţinerii realizate de agenţi externi, întreţinerii de la distanţă şi lucrului realizat prin intermediul mijloacelor electronice de comunicare. Există o modalitate adecvată de distrugere/eliminare a documentelor şi suporturilor de date (ca de exemplu, distrugătoare de documente, coşul de protecţie a datelor) implementată de întreprinderi de încredere care au ca obiect de activitate distrugerea de documente.

Conceptul de rol/autorizare va fi adaptat în mod regulat la structurile organizaţiei de lucru care suferă modificări (de exemplu, roluri noi), iar rolurile/autorizările atribuite vor fi revizuite la intervale regulate de timp (de exemplu, de către superiorul ierarhic) pentru a fi ajustate sau revocate, în cazul în care acest lucru este necesar. Există un control centralizat regulat în ceea ce priveşte profilurile standard atribuite. Accesările modificate permanent (scriere, ştergere) vor fi înregistrate, iar fişierele de logare generate vor fi păstrate pentru o perioadă adecvată de timp (cel puţin 90 de zile) şi vor fi verificate (aleatoriu).

Pentru asigurarea siguranţei generale a transferului de date vor fi luate mai multe măsuri standard:

Persoanele însărcinate cu transferul datelor vor fi informate în prealabil cu privire la măsurile de precauţie care trebuie să fie luate. Destinatarii transferului de date vor fi stabiliţi în prealabil, astfel încât să fie posibilă efectuarea unui control (autentificare) corespunzător. Procesul global de transferare a datelor trebuie să fie specificat şi documentat, iar implementarea transferului de date va fi înregistrată, respectiv documentată (de exemplu, confirmare de primire, confirmare). Persoanele însărcinate cu transferul datelor vor efectua în prealabil o verificare a plauzibilităţii, caracterului integral şi corectitudinii datelor.

Înainte de efectuarea transferului datelor se va realiza o verificare a adresei destinatarului (de exemplu, adresa de e-mail). Transferul de date realizat prin intermediul Internetului are loc în formă criptată (de exemplu, prin criptarea fişierelor). În cazul în care acest lucru este posibil din punct de vedere tehnic, integritatea datelor transferate va fi asigurată prin utilizarea procedurilor de semnătură (semnătură digitală). Confirmările electronice trebuie să fie arhivate în mod corespunzător. Transferurile accidentale de date prin intermediul Internetului vor fi evitate prin utilizarea unor tehnologii adecvate (de exemplu proxy, firewall).

În plus, pentru punerea în aplicare a cerinţei de separare vor fi luate următoarele măsuri standard:

Există reglementări obligatorii cu privire la scopul prelucrării datelor pentru a asigura astfel respectarea cerinţei de separare. Datele colectate în scopuri specifice vor fi stocate separat de datele colectate în alte scopuri. Sistemele informatice utilizate permit stocarea separată a datelor (prin capabilităţi multi-client sau concepte de acces). Există o separare a datelor în cadrul sistemelor de testare şi producţie. În cazul datelor pseudonimizate, puntea cheie care permite reidentificarea este salvată, respectiv păstrată separat. În cazul prelucrării datelor cu

caracter personal sau transferului de funcţii, datele diferiţilor beneficiari vor fi prelucrate separat de către contractant. Conceptele de rol/autorizare existente permit, datorită modalităţii în care acestea sunt concepute, separarea logică a datelor prelucrate.

4. Asigurarea integrităţii

Pentru efectuarea înregistrării intrărilor vor fi luate mai multe măsuri standard:

Vor fi înregistrate toate modificările aduse drepturilor de acces şi activităţilor de administrator. Vor fi înregistrate toate accesările în scris (intrări, modificări, ştergeri) şi modificările câmpurilor de date (de exemplu, conţinutul înregistrării recent introduse sau modificate). Va fi realizată înregistrarea tuturor transferurilor de date (de exemplu, descărcări de date) şi a tuturor activităţilor de logare.

Documentele de înregistrare utilizate sunt documentate şi arhivate pentru a asigura astfel trasabilitatea intrărilor. Înregistrarea în jurnal se face împreună cu precizarea datei şi orei, utilizatorului, tipului de activitate, programului de aplicaţie şi numărului de ordine al înregistrării. Setările pentru înregistrarea în jurnal trebuie să fie documentate.

Pentru fişierele de logare se permite numai accesul de citire. Grupul persoanelor autorizate cu privire la accesarea fişierelor de logare este limitat (acesta poate fi limitat, de exemplu, la administrator, responsabilul pentru protecţia datelor, auditor). Fişierele de logare vor fi păstrate pentru o anumită perioadă de timp (de exemplu, 1 an), iar apoi vor fi şterse, cu respectarea dispoziţiilor de confidenţialitate. Fişierele de logare sunt evaluate automat, la anumite intervale regulate de timp. Evaluările fişierelor de logare vor fi create, pe cât posibil, într-o formă pseudonimizată.

5. Asigurarea disponibilităţii

Arhitectura este asigurată de la sine în cadrul platformei AWS împotriva pierderii datelor, cu ajutorul unor mecanisme interne de replicare. În plus, pentru asigurarea securităţii obiectelor vor fi luate următoarele măsuri standard AWS:

Vor fi luate toate măsurile necesare privind protecţia împotriva incendiilor (de exemplu, uşi de incendiu, avertizoare de fum, pereţi de incendiu, interzicerea fumatului). Sistemele informatice vor fi protejate împotriva inundaţiilor (de exemplu, sala de calculatoare se va afla la etajul 1, detector de apă). Vor fi luate măsuri pentru a preveni şocurile mecanice puternice (de exemplu, sala de calculatoare nu trebuie să se afle în apropierea drumurilor principale, trenurilor, sălilor de maşini). Sistemele informatice vor fi protejate împotriva câmpurilor electromagnetice (de exemplu, prin montarea unor panouri de oţel în pereţii exteriori). Vor fi luate măsuri pentru prevenirea actelor de vandalism şi furturilor (a se vedea Controlul accesului). Sistemele informatice sunt instalate în spaţii dotate cu aparate de aer condiţionat (temperatura şi umiditatea sunt controlate cu ajutorul aparatelor de aer condiţionat). Sistemele informatice sunt protejate împotriva vârfurilor de supratensiune cu ajutorul unor echipamente de protecţie la supratensiune. Vor fi luate măsuri pentru a asigura o alimentare

continuă cu energie electrică şi cu nivel redus de zgomot (de exemplu, prin montarea unor surse UPS, generatoare de urgenţă).

Datele sunt copiate în mod regulat sunt forma unor copii de rezervă în cadrul platformei AWS. Conceptul privind asigurarea copiilor de rezervă este documentat, revizuit şi actualizat în mod regulat. Copiile de rezervă sunt protejate împotriva accesului neautorizat. Programele utilizate pentru realizarea copiilor de rezervă respectă standardele actuale de calitate şi sunt actualizate periodic. Este amenajat un centru pentru datele de redundanţă (amplasat la o anumită distanţă de locaţia unde are loc procesarea datelor), iar acesta poate continua procesarea datelor în cazul unor calamităţi naturale. Diferitele măsuri de control pentru asigurarea disponibilităţii sunt documentate de AWS în cadrul unui plan de gestionare a situaţiilor de urgenţă.

Înainte de acordarea unui contract pentru prelucrarea datelor cu caracter personal va fi efectuată o verificare amănunţită a contractantului în conformitate cu criteriile stabilite (măsuri tehnice şi organizatorice). Pentru aceasta, este necesară descrierea şi verificarea detaliată a măsurilor tehnice/organizaţionale privind protecţia datelor întreprinse de contractant (prin răspunderea la un chestionar sau prin elaborarea unui concept de protecţie a datelor). În funcţie de cantitatea şi de cât de sensibile sunt datele prelucrate, această verificare poate fi efectuată şi la sediul contractantului. La selectarea contractanţilor vor fi luate în considerare certificările corespunzătoare (de exemplu, ISO 27001). Stabilirea adecvării contractantului trebuie să fie documentată într-o formă adecvată şi inteligibilă.

Pentru stabilirea relaţiei contractuale, beneficiarul şi contractantul vor încheia împreună un acord privind prelucrarea datelor cu caracter personal. Acesta specifică detaliat şi în scris competenţele şi responsabilităţile, precum şi obligaţiile care le revin celor două părţi contractuale. În cazul în care un prestator de servicii contractat are sediul în afara UE sau în afara SEE, se aplică clauzele contractuale standard ale UE. Contractul stipulează că prelucrarea datelor de către contractant poate avea loc numai în conformitate cu instrucţiunile beneficiarului. Contractantul este obligat să informeze imediat beneficiarul în cazul în care acesta consideră că o anumită instrucţiune primită din partea beneficiarului încalcă Legislaţia europeană privind protecţia datelor cu caracter personal. Pentru a asigura respectarea drepturilor persoanelor vizate, în contractul de prelucrare a datelor cu caracter personal este stipulat ca contractantul să ofere beneficiarului toată susţinerea de care acesta are nevoie, în cazul în care acest lucru este necesar, de exemplu, cu ocazia furnizării de informaţii persoanelor vizate.

În cadrul procesului de prelucrare a datelor cu caracter personal, beneficiarul va verifica rezultatele activităţii prestate de contractant cu privire la forma şi conţinutul acesteia. Se va verifica periodic respectarea măsurilor tehnice şi organizatorice întreprinse de contractant. Această cerinţă va fi îndeplinită, în primul rând, prin prezentarea documentelor actuale de testare, respectiv a certificatelor adecvate sau a documentelor doveditoare referitoare la auditul de securitate informaţională sau de confidenţialitate efectuat. În măsura în care sunt angajaţi subcontractanţi, în contract se va stipula controlarea corespunzătoare a acestora.

6. Asigurarea capacității sistemelor

Infrastructura AWS bazată pe tehnologia cloud a fost creată ca fiind una dintre cele mai flexibile și mai sigure medii de cloud computing. Această infrastructură a fost proiectată pentru o disponibilitate optimă, cu o separare completă a beneficiarilor. Aceasta pune la dispoziție o platformă foarte scalabilă, extrem de fiabilă, care permite beneficiarilor să implementeze rapid și sigur aplicații și conținuturi în întreaga lume, conform necesităților acestora. Serviciile AWS sunt independente de conținut și oferă tuturor clienților același nivel ridicat de securitate, indiferent de tipul de conținut sau de regiunea geografică unde este stocat conținutul respectiv.

Centrele de Date AWS de clasă mondială și extrem de sigure utilizează sisteme de supraveghere electronică de ultimă generație și sisteme de control al accesului pe mai multe niveluri. Centrele de Date dispun în permanență de personal de securitate instruit, iar accesul este acordat strict în conformitate cu principiul privind acordarea a cât mai puține drepturi și doar în scopul asigurării administrării sistemului.

7. Proceduri de restabilire a disponibilității datelor cu caracter personal în urma unui incident fizic sau tehnic

Centrele de date AWS sunt construite în clustere aflate în diferite regiuni ale lumii. Toate centrele de date sunt online și deservesc clienții; toate centrele de date funcționează în permanență. În caz de avarie, o serie de procese automate vor comuta traficul clienților departe de zonele afectate. Aplicațiile de bază sunt implementate pe baza unei configurații N+1, astfel încât, în cazul unei avarii a centrului de date, să existe o capacitate suficientă pentru a putea direcționa în mod echilibrat traficul de date către celelalte locații.

AWS vă oferă posibilitatea de a plasa în mod flexibil anumite entități și de a stoca date în mai multe regiuni geografice, precum și prin intermediul mai multor Availability Zones. Fiecare Availability Zone a fost dezvoltată ca zonă de avarie independentă. Aceasta înseamnă că Availability Zones sunt distribuite fizic într-o regiune tipică a orașului și, prin urmare, că sunt situate, de exemplu, în zone cu risc scăzut de inundații (în funcție de regiune, există diferite categorii de zone de inundații). Pe lângă sursa autonomă neîntreruptibilă de alimentare cu curent electric și generatoarele de rezervă prezente fața locului, toate Availability Zones sunt alimentate de furnizori independenți de energie electrică prin intermediul mai multor rețele electrice diferite, pentru a minimiza astfel numărul locațiilor afectate în cazul producerii unei avarii. Toate Availability Zones sunt conectate redundant la mai mulți furnizori de tranzit de nivel 1.

Echipa Amazon însărcinată cu gestionarea incidentelor aplică proceduri de diagnosticare standard pentru a ajuta la rezolvarea incidentelor comerciale critice. Operatorii oferă o acoperire continuă, 24x7, șapte zile pe săptămână, 365 de zile pe an, pentru detectarea eventualelor incidente și pentru gestionarea și remedierea acestora.

8. Proceduri de revizuire periodică, de anticipare şi de evaluare a eficacităţii măsurilor tehnice şi organizatorice

Politicile şi instrucţiunile existente ale companiei, respectiv standardele implementate în materie de securitate a informaţiilor se aplică şi în cazul implementării şi funcţionării platformei RIO. Sunt disponibile funcţii operaţionale pentru protecţia datelor şi securitatea informaţiilor (responsabilul cu protecţia datelor şi Information Security Officer). Angajaţii se obligă să păstreze confidenţialitatea datelor, iar aceştia vor fi informaţi cu privire la măsurile necesare referitoare la securitatea datelor sau securitatea IT prin intermediul unor broşuri, pliante, informaţii transmise prin Intranet etc.

Procesele interne sunt verificate cu privire la respectarea măsurilor tehnice şi organizatorice necesare pentru asigurarea securităţii datelor prin activităţi de revizuire, de securitatea informaţiei şi de protecţia datelor.

Operaţiunile de prelucrare a datelor şi măsurile de securitate a datelor sunt documentate în cadrul unui director care conţine activităţile de prelucrare date. Se va efectua o verificare periodică (internă şi externă) privind eficienţa măsurilor întreprinse.