LOGISTIK IM FLUSS.

Zmluva o spracovaní osobných údajov (podľa čl. 28 všeobecného nariadenia o ochrane osobných údajov)

medzi

užívateľom (ako je definované v hlavnej zmluve)

(ďalej len ako **„zadávateľ zákazky“**)

a

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

(ďalej len ako **„príjemca zákazky“**)
(zadávateľ a príjemca zákazky ďalej len ako **„Zmluvná strana“** spolu ako **„Zmluvné strany“**).

Preambula

(A) Túto zmluvu o spracovaní údajov (ďalej len „**zmluva**“) možno použiť na všetky činnosti, pri ktorých príjemca zákazky prichádza do styku s osobnými údajmi zadávateľa zákazky (ako je definované dolu pod číslicou 1.5), iného poskytovateľa alebo iných dotknutých osôb v súvislosti s činnosťou vyplývajúcou zo všeobecných rámcových podmienok k základnému užívaniu popísanou pod číslicou 2 a prípadne na jednotlivé zmluvy uzatvorené pre ďalšie služby (ďalej len ako „**hlavná zmluva**“).

(B) Na základe tejto zmluvy koná zadávateľ zákazky ako zodpovedná osoba a príjemca zákazky ako spracovateľ zákazky v rámci spracovania údajov o zákazke podľa čl. 28 všeobecného nariadenia o ochrane osobných údajov (ako je definované nižšie).

Zmluvné strany sa dohodli na nasledujúcom:

1 Definície a interpretácia

1.1 „**Európske právo**“ je právo aplikovateľné v rámci Európske únie, zákony aplikovateľné v súčasných členských štátov Európskej únie ako aj zákony aplikovateľné v rámci každého štátu, ktorý sa dodatočne stane členským štátom Európskej únie.

1.2 „**Európske právo na ochranu údajov**“ je aplikovateľné právo v rámci Európskej únie na spracovanie osobných údajov (obzvlášť GVO ochrana údajov), zákony na spracovanie osobných údajov (predovšetkým Zákon o ochrane údajov v súčasne platnom znení) aplikovateľné v súčasných členských štátov Európskej únie ako aj zákony na spracovanie osobných údajov aplikovateľné v rámci každého štátu, ktorý sa dodatočne stane členským štátom Európskej únie.

1.3 „**GVO - ochrana údajov**“ je „NARIADENIE (EU) 2016/679 EURÓPSKEHO PARLAMENTU A RADY zo dňa 27. Apríla 2016 na ochranu fyzických osôb pri spracovaní osobných údajov, pre voľný pohyb údajov a pre zrušenie smernice 95/46/EH (Základná vyhláška na ochranu údajov)“.

1.4 „**Zákon na ochranu údajov**“ je Spolkovým zákonom na ochranu údajov.

1.5 „**Osobné údaje**“ majú význam, aký je uvedený v Zákone na ochranu údajov / v GVO ochrane údajov.

2 Predmet spracovania údajov/povinnosti zadávateľa zákazky

2.1 Táto zmluva upravuje povinnosti zmluvných strán v súvislosti so spracovaním osobných údajov zadávateľa zákazky prostredníctvom príjemcu zákazky v rámci hlavnej zmluvy uvedenej v Prílohe 1.

2.2 Predmet a dĺžka spracovania, druh a účel spracovania, druh osobných údajov, kategórie dotknutých osôb a povinnosti a práva zodpovednej osoby vyplývajú z Prílohy 1 tejto zmluvy a z popisu služieb hlavnej zmluvy.

2.3 Zadávateľ zákazky zostáva na základe všeobecného nariadenia o ochrane osobných údajov zodpovednou osobou a zaručuje prípustnosť spracovania osobných údajov dotknutých osôb (vodiča a prípadných ďalších osôb). V tejto súvislosti si zadávateľ zákazky plní najmä svoju rozsiahlu informačnú povinnosť a zabezpečí, že na účely spracovania osobných údajov predloží právne podklady v súlade so zákonom o ochrane osobných údajov (napr. uzatvorenie dohody o prevádzke, obmedzenie spracovania na účely zamestnaneckého pomeru).

3 Povinnosti príjemcu zákazky

3.1 Príjemca zákazy spracúva osobné údaje o zadávateľovi zákazky výlučne na účely uvedené v Prílohe 1, v rámci hlavnej zmluvy, ako aj v zákazke a podľa pokynov zadávateľa uvedených v Prílohe 1; príjemca zákazky nemôže spracovať osobné údaje na základe tejto zmluvy na žiadne iné účely. Spracovanie údajov mimo tejto zmluvy pre vlastné účely podľa čísla 8.3.4 Hlavnej zmluvy zostáva týmto nedotknuté. Kópie alebo duplikáty osobných údajov sa nesmú vyhotovovať bez vedomia zadávateľa zákazky. Výnimku z toho tvoria zálohy, pokiaľ sú požadované na zabezpečenie riadneho spracovania údajov, ako aj údajov, ktoré sú potrebné na dodržanie zákonných povinností na archiváciu údajov.

3.2 Po ukončení spracovania údajov má príjemca zákazky povinnosť buď odovzdať a/alebo na základe práva o ochrane údajov vymazať všetky osobné údaje zadávateľa zákazky podľa jeho výberu, pokiaľ tomu neodporuje žiadna zákonná lehota na archiváciu údajov a pokiaľ ich nespracúva príjemca zákazky na vlastné účely mimo tejto zmluvy podľa číslice 8.3.4. hlavnej zmluvy. To isté platí pre testovací a odpadový materiál. Celkové vymazanie príp. vydanie údajov zadávateľovi musí byť na základe jeho žiadosti potvrdené aj s uvedením dátumu.

3.3 Pokiaľ je to v rozsahu poskytnutých služieb, podporuje príjemca zákazky zadávateľa zákazky pri plnení práv dotknutých osôb (informácie, oprava, nesúhlas, vymazanie) podľa príslušných pokynov zadávateľa zákazky.

3.4 Príjemca zákazky potvrdí, že – pokiaľ je to zákonom požadované – určil osobu poverenú na ochranu údajov (porovnaj § 38 nemeckého Zákona na ochranu údajov s čl. 37 európskeho všeobecného nariadenia o ochrane osobných údajov).

3.5 Príjemca je povinný, bezodkladne informovať zadávateľa o výsledku kontroly úradov vykonávajúcich dozor nad ochranou dát, pokiaľ tieto súvisia so spracovaním údajov o zadávateľovi. V prípade zistených nedostatkov, ich prijímateľ v primeranej lehote odstráni a upovedomí o tom zadávateľa.

3.6 Spracovanie údajov prijímateľom zákazky a subdodávateľmi poverenými zadávateľom zákazky sa ková výlučne na území Spolkovej republiky Nemecko, v členskom štáte Európskej únie alebo v inom zmluvnom štáte Dohovoru o Európskom Hospodárskom priestore. Každé premiestnenie do inej krajiny (ďalej len „**tretia krajina**“) vyžaduje predchádzajúci výslovný súhlas zadávateľa zákazky a smie sa uskutočniť len vtedy, ak sú splnené osobitné predpoklady na export údajov do tretích krajín (porovnaj čl. 40 a násl. všeobecného nariadenia o ochrane osobných údajov). K tomu sú požadované údaje uvedené v Prílohe 1, príp. je potrebné doplniť príslušné (zmluvné) podklady.

3.7 Príjemca zákazky je povinný oboznámiť zamestnancov poverených na vykonávanie prác so smerodajnými ustanoveniami na ochranu údajov a tí sú povinní dodržiavať mlčanlivosť o týchto údajoch (porovnaj čl. 28 všeobecného nariadenia na ochranu osobných údajov, ods. 3b)), ako aj zabezpečiť vhodnými krokmi to, že každý zamestnanec bude spracovávať osobné údaje iba podľa pokynov zadávateľa zákazky.

3.8 Príjemca zákazky pravidelne kontroluje dodržiavanie právnych predpisov tejto zmluvy a zdokumentované pokyny zadávateľa počas celej doby platnosti zmluvy. Výsledky kontrol sa musia na požiadanie zadávateľa predložiť, pokiaľ sú tieto relevantné na spracovanie údajov o zadávateľovi. Opatrenia na kontrolu sú popísané v koncepte na ochranu údajov, ktorý sa musí predložiť zadávateľovi na jeho vyžiadanie.

3.9 Prijímateľ musí pritom poskytovať zadávateľovi podporu so zreteľom na druh spracovania a podľa možností vhodnými technickými a organizačnými opatreniami, a plniť si svoju povinnosť, dodržiavať práva dotknutých osôb popísaných v kapitole III GVO ochrany údajov. Zadávateľ hradí všetky náklady, ktoré pritom vzniknú prijímateľovi.

3.10 Prijímateľ zákazky je povinný poskytovať zadávateľovi podporu vzhľadom na druh spracovania a informácie, ktoré má k dispozícii, pri súčasnom dodržiavaní povinností uvedených v článku 32 až 36 GVO ochrany údajov.

4 Technické a organizačné opatrenia na zabezpečenie údajov

4.1 Príjemca vykoná primerané technické a organizačné opatrenia na ochranu údajov (porovnaj čl. 32 všeobecného nariadenia na ochranu osobných údajov). Prijímateľ je zvlášť povinný aplikovať technické a organizačné opatrenia dohodnuté v Prílohe 2 tejto zmluvy. Tieto opatrenia musí prijímateľ zákazky prispôsobiť v priebehu zákazky ďalšiemu technickému a organizačnému vývoju, aby pritom neklesla úroveň ochrany. Podstatné zmeny je potrebné dohovoriť písomne.

4.2 Prijímateľ preukáže zadávateľovi zákazky na jeho žiadosť vecné dodržiavanie technických a organizačných opatrení.

4.3 Prijímateľ je povinný viesť zodpovedajúcu dokumentáciu spracovaných údajov, na základe ktorej môže zadávateľ podať dôkaz o riadnom spracovaní údajov. Dôkaz možno podať aj prostredníctvom povoleného certifikačného konania podľa článku 42 GVO ochrany údajov.

5 Subdodávatelia

5.1 Prijímateľovi zákazky sa týmto povoľuje zapojenie subdodávateľa menovaného v Prílohe 1.

5.2 Týmto sa generálne povoľuje zapojenie ďalších subdodávateľov. Prijímateľ zákazky informuje zadávateľa o každej zamýšľanej zmene so zreteľom na prizvanie alebo náhradu subdodávateľmi; zadávateľ môže podať odvolanie voči zamýšľaným zmenám. Tieto služby nemožno chápať ako vzťahy subdodávok v zmysle tejto úpravy, ktoré prijímateľ zákazky požaduje u tretích osôb ako vedľajšiu službu na podporu realizácie zákazky. K tomu sa pripočítavajú napr. telekomunikačný služby, čistiace sily, kontrolóri alebo likvidácia nosičov údajov. Prijímateľ zákazky je však povinný, na zabezpečenie ochrany a bezpečnosti údajov zadávateľa prijať pri externom dodávaní vedľajších služieb primerané a zákonne zmluvné dohody ako aj kontrolné opatrenia.

5.3 Ak príjemca zákazky požaduje subdodávateľa, príjemca zákazky musí zabezpečiť, aby mu boli uložené na základe (i) uzavretej zmluvy medzi subdodávateľom a príjemcom zákazky alebo (ii) iných právnych prostriedkov podľa Európskeho práva na ochranu údajov tie isté povinnosti na ochranu údajov, aké sú uložené príjemcovi zákazky podľa tejto zmluvy. Pritom musí príjemca zákazky obzvlášť zabezpečiť, aby subdodávateľ ponúkol dostatočné záruky na vykonanie vhodných technických a organizačných oparení, aby sa spracovanie osobných údajov uskutočnilo zodpovedajúco požiadavkám podľa všeobecného nariadenia na ochranu osobných údajov. Na písomnú žiadosť zadávateľa poskytne prijímateľ zadávateľovi informáciu ohľadom podstatného obsahu zmluvy a vykonania povinností relevantných na ochranu údajov v rámci subdodávkového vzťahu, v prípade, že je to nutné, aj prostredníctvom náhľadu do relevantných zmluvných podkladov. Komerčné podmienky môžu pritom prijímateľa zákazky poškodiť. Objednávateľ je povinný dodržiavať mlčanlivosť ohľadom získaných informácii.

6 Práva na kontrolu

6.1 Zadávateľ zákazky má právo kontrolovať dodržiavanie povinností vyplývajúcich z tejto zmluvy (vrátane udelených pokynov) sám alebo prostredníctvom tretích osôb menovaných zadávateľom príp. si nechať skontrolovať ich dodržiavanie.

6.2 Prijímateľ zákazky zaručuje zadávateľovi zákazky poskytovať pri kontrole primeranú podporu. Predovšetkým prijímateľ zákazky zaručuje prístup k zariadeniam na spracovanie údajov a poskytuje požadované informácie.

6.3 V prípade, že kontrola zistí výsledok, že prijímateľ zákazky a/alebo spracovateľ nedodržiava predpisy tejto zmluvy a/alebo európske právo na ochranu údajov, prijímateľ zákazky vykoná všetky opravné opatrenia, ktoré sú požadované, aby sa zaručilo dodržiavanie predpisov tejto zmluvy a/alebo predpisov európskeho práva na ochranu údajov.

6.4 Náklady, ktoré zadávateľovi vzniknú pri výkone kontroly, si zadávateľ hradí sám. Náklady, ktoré vzniknú príjemcovi zákazky pri výkone kontroly zadávateľom, môže požadovať od zadávateľa, pokiaľ zadávateľ vykonáva kontrolu viac ako raz v kalendárnom roku, príp. si ju nechá vykonať.

6.5 Kontroly vedené u prijímateľa zákazky sa musia včas oznámiť a nesmú neprimerane obmedziť prevádzku u príjemcu zákazky.

7 Povinnosť na upozornenie

Príjemca zákazky bezodkladne informuje zadávateľa, ak niektorý z pokynov udelených zadávateľom, podľa mienky príjemcu, porušuje európske právo na ochranu údajov. Pokyn, ktorý odporuje právu, nemusí byť dodržaný, pokiaľ nie je zadávateľom zmenený alebo výslovne potvrdený. Prijímateľ zákazky nie je povinný vykonať materiálno-právnu kontrolu pokynov.

Prijímateľ zákazky musí bezodkladne informovať zadávateľa zákazky, ak zistí chyby alebo odchýlky pri spracovaní údajov alebo ak má podozrenie na porušenie ochrany údajov (a z toho vyplývajúci „**Incident**“). Zadávateľ zákazky musí prípad zdokumentovať vrátane všetkých vecných udalostí, ich dôsledkov a všetkých opatrení na ich odstránenie a na požiadanie zadávateľa tieto zdokumentované informácie bezodkladne písomne alebo elektronicky odovzdať zadávateľovi.

8 Ručenie a uvoľnenie

8.1 Príjemca zákazky ručí za škody, ktoré boli spôsobené úmyselne a/alebo hrubou nedbanlivosťou zo strany príjemcu alebo jeho poverencami. Za škody, ktoré sa zakladajú na drobnej nedbanlivosti príjemcu alebo jeho poverencov, ručí príjemca len vtedy, pokiaľ je porušená kardinálna povinnosť. Kardinálne povinnosti sú podstatné zmluvné povinnosti, ktoré umožňujú riadnu vykonateľnosť zmluvy a na ktorých

splnenie bol poverený zadávateľ zákazky. Pri drobnej nedbanlivosti, ktoré vedú k porušeniu takýchto kardinálnych povinnosti, je ručenie príjemcu zákazky so zreteľom na typické predvídateľné škody ohraničené.

8.2 Zadávateľ zákazky zbaví príjemcu všetkých nárokov tretích osôb (vrátane dotknutých osôb a/alebo úradov na ochranu údajov), škôd a nákladov, ktoré sa zakladajú na porušení zo strany zadávateľa voči ustanoveniam tejto zmluvy a/alebo voči Európskemu právu na ochranu dát: to neplatí, pokiaľ zadávateľ porušenie nespôsobil alebo pokiaľ príjemca prispel k tomuto porušeniu.

9 Splatnosť

Splatnosť tejto zmluvy zodpovedá splatnosti hlavnej zmluvy. Po ukončení hlavnej zmluvy z akéhokoľvek dôvodu sa táto zmluva tiež automaticky ukončí. Výpoveď z dôležitého dôvodu zostáva nedotknutá.

10 Ostatné

10.1 Služby príjemcu zákazky podľa tejto zmluvy sa uhradia na základe pravidla odmeňovanie upraveného v Hlavnej zmluve.

10.2 V prípade ohrozenia osobných údajov zadávateľa u príjemcu zákazky prostredníctvom opatrení tretích osôb (napr. exekúcia alebo konfiškácia), insolvenciou alebo vyrovnávacím konaním alebo prostredníctvom iných porovnateľných udalostí, musí o tom príjemca zákazky bezodkladne informovať zadávateľa zákazky.

10.3 V prípade neúčinnosti jednotlivých ustanovení tejto zmluvy, sa toto nedotkne účinnosti zvyšných ustanovení. Zmluvné strany dohodnú v prípade neúčinnosti niektorej klauzuly náhradnú právnu úpravu zameranú na vecný a hospodársky účel zmluvy.

10.4 V prípade, ak Veľká Británia vystúpi z Európskej únie, príjemca zákazky sa zaväzuje, už teraz ukončiť všetky dohody a vykonať všetky opatrenia, ktoré sú požadované na spracovanie údajov týkajúcich sa predmetu zmluvy vo Veľkej Británii od doby jej vystúpenia podľa práva na ochranu údajov. Pokiaľ nebude do doby vystúpenia predložené žiadne pozitívne rozhodnutie Európskej komisie, nahradzujú ho zo súčasného pohľadu osobitné klauzuly štandardnej ochrany údajov podľa článku 46 ods. 2 c) na prenos osobných údajov na spracovateľa zákazky, ktoré sú zastúpené v tretích krajinách, v ktorých nie je zaručená žiadna úroveň ochrany.

Pokiaľ príjemca zákazky nedodrží tieto povinnosti, je zadávateľ zákazky oprávnený, požadovať od príjemcu zákazky s účinnosťou od doby vylúčenia Veľkej Británie z Európskej únie, aby dotknuté služby boli dodané od príbuznej firmy príp. časťou podniku so stálym sídlom na území Európskej únie, bez toho, aby zadávateľovi vznikli dodatočné náklady.

10.5 Táto zmluva o spracovaní osobných údajov je k dispozícii v 18 jazykoch, pričom nemecké originálne znenie má v prípade odchýlok prednosť pred ostatnými jazykmi.

10.6 Táto zmluva podlieha právu Spolkovej republike Nemecko pri vylúčení obchodného práva OSN. Výlučná príslušnosť súdu je v Mníchove.

10.7 Súčasťou zmluvy sú nasledujúce prílohy:

Príloha 1 – Popis spracovania zákazky
Príloha 2 - Technické a organizačné opatrenia

PRÍLOHA 1 – Popis spracovania zákazky

1 Hlavná zmluva

Hlavnou zmluvou v zmysle číslice 2.1 hlavnej časti zmluvy sú „Všeobecné rámcové podmienky k základnému užívaniu“.

Titul - Zmluvné strany: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 München/**užívateľ**

2 Predmet a trvanie zákazky

Predmet zákazky vyplýva z číslice 1 (*predmet zmluvy*) a číslice 8 (*údaje užívateľa a ochrana údajov)* hlavnej zmluvy; trvanie zákazky vyplýva z číslice 7 (*uzavretie zmluvy, trvanie zmluvy a práva výpovede*) Hlavnej zmluvy.

3 Rozsah, druh a účel spracovania údajov / opatrenia na spracovanie údajov

Rozsah, druh a účel spracovania osobných údajov vyplývajú z číslice 8 hlavnej zmluvy.

Bližší popis predmetu zákazky so zreteľom na rozsah, druh a účel:

Aby mohol príjemca zákazky poskytnúť ponúkané služby (ako je definované v hlavnej zmluve), musí príjemca zákazky poskytnúť osobné údaje o zadávateľovi zákazky prostredníctvom Connected Vehicles alebo Mobile Devices (a príp. o treťom poskytovateľovi, s ktorým užívateľ dohodol ďalšie služby, prenesené osobné údaje) v miere požadovanej na poskytovanie služieb a preniesť ich na platformu príjemcu zákazky a tam uložiť. Príjemca zákazky spracuje údaje uložené na platforme v rozsahu požadovanom pre poskytnutie služieb (napr. analyzovať a vyhodnocovať na základe osobných údajov jazdné vlastnosti vodičov, ako aj užívanie Connected Vehicle alebo Mobile Device a predložiť zadávateľovi zákazky špeciálne pre neho vyhradené ponuky, ako sú tréningy vodičov, detaily vybavenia, ako aj návrhy na zvýšenie efektívnosti). Presný rozsah, druh a účel vyplývajú predovšetkým z dodatočne uzatvorených samostatných zmlúv.

4 Okruh dotknutých osôb (kategórie dotknutých osôb)

Spracovanie osobných údajov sa týka nasledujúcich okruhov osôb:

- **Vodiči a ostatní zamestnanci** (zamestnanci vlastnej spoločnosti zadávateľa zákazky), napr. zamestnanci, študujúci, uchádzači, bývalí zamestnanci;
- **Vodiči**, ktorí nie sú zamestnancami;
- **Kontaktné osoby** pre nakladačov/vykladačov alebo iných obchodných partnerov zadávateľa zákazky; a
- **Zamestnanec koncernu** (zamestnanec inej skupinovej spoločnosti zadávateľa zákazky).

5 Druh osobných údajov

Spracovanie osobných údajov zahŕňa nasledujúci okruh osobných údajov:

- Meno vodiča a identifikačné číslo vodiča;
- Identifikačné číslo vozidla;
- Údaje o lokalite;
- Údaje o dobe šoférovania a dobe oddychu;
- Údaje o jazdných vlastnostiach;
- Údaje o stave Connected Vehicle;
- Údaje o stave prívesu;
- Údaje o stave nadstavby príp.prístavby, agregátov a ďalších súčastí vozidla;
- Údaje o stave príp. pripojených IOT-Devices
- Údaje o stave Mobile Devices;
- Údaje o náklade;
- Údaje o zákazke;
- Údaje na kontaktné osoby pre nakladačov/vykladačov alebo iných obchodných partnerov zadávateľa zákazky.

6 Zdokumentované pokyny

Zadávateľ zákazky týmto poučuje príjemcu zákazky o tom, aby spracoval osobné údaje, ako je uvedené v číslici 8 hlavnej zmluvy. To zahŕňa predovšetkým nasledujúce spracovanie:

- Osobné údaje sa prenášajú cez Connected Vehicle alebo Mobile Device na cloudovú platformu príjemcu zákazky a tam sa ukladajú.
- Osobné údaje sa spracúvajú na základe tejto zmluvy, pokiaľ je to požadované na naplnenie hlavnej zmluvy; číslica 8.3.4 tejto hlavnej zmluvy zostáva tým nedotknutá.
- Príjemca zákazky prenáša osobné údaje na tretieho poskytovateľa (ako je definované v hlavnej zmluve), pokiaľ je takýto prenos na tretieho poskytovateľa požadovaný, aby tento svoje služby (ako je definované v hlavnej zmluve) mohol poskytnúť zadávateľovi zákazky.
- Príjemca zákazky analyzuje a vyhodnocuje na základe osobných údajov jazdné vlastnosti vodičov, ako aj použitie Connected Vehicles a predkladá zadávateľovi zákazky špeciálne pre neho určené ponuky, ako sú tréningy vodičov, detaily vybavenia, ako aj návrhy na zvýšenie efektívnosti.

7 Miesto spracovania

- Nemecko
- Spojené Kráľovstvo; pokiaľ sa údaje spracúvajú na účely IT hostingu a/alebo IT supportu v rámci Európskej únie, uzatvoria sa príslušné zmluvy o spracovaní osobných údajov.

- Pokiaľ príjemca zákazky použije k IT hostingu a/alebo na účely IT supportu subdodávateľov mimo Európskej únie (k tomu pozri číslicu 8 tejto Prílohy 1), uskutoční sa postúpenie osobných údajov na základe medzi príjemcom zákazky a subdodávateľom uzatvorených štandardných zmluvných klauzúl/štandardných klauzúl o ochrane údajov na účely prenosu osobných údajov na spracovateľa zákazky do tretích krajín podľa čl. 46 ods. 2 c) všeobecného nariadenia o ochrane osobných údajov.

8 Subdodávatelia

Príjemca zákazky využije nasledujúcich subdodávateľov (ktorí využijú príp. ďalších subdodávateľov):

Číslo	Subdodávateľ (firma, adresa, kontaktná osoba)	Spracované kategórie údajov	Kroky na spracovanie údajov/účel spracovania subdodávok
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Všetky osobné údaje platformy, ktoré sa týkajú časti predaja (t. j. kde sa môže zákazník na platforme registrovať a realizovať objednávky)	Hosting platformy
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Všetky osobné údaje platformy, ktoré sa týkajú časti predaja (t. j. kde sa môže zákazník na platforme registrovať a realizovať objednávky)	IT Support ohľadom platformy
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 USA https://aws.amazon.com/de/compliance/contact/	Všetky ostatné osobné údaje užívateľa, ktoré sa prenášajú prostredníctvom vozidla príjemcovi zákazky	Hosting platformy / IT-Support ohľadom hosting platformy
4	Príp. v budúcnosti namiesto č. 3: Amazon Webservices (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 USA https://aws.amazon.com/de/compliance/contact/	Všetky ostatné osobné údaje užívateľa, ktoré sa prenášajú prostredníctvom vozidla príjemcovi zákazky	Hosting platformy
5	MAN Service a Support GmbH Dachauer Str. 667	Všetky osobné údaje, ktoré sú požadované na spracovanie otázok zákazníka v rámci 1. a 2. úrovne	1. úroveň podpory

	80995 München Nemecko	podpory	
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 USA	Všetky osobné údaje, ktoré sú požadované na vystavenie faktúr/vybavenie zákazky sú	Hosting platformy (EU Tenant – Gehosted by Amazon Web Services (EU) – pozri číslicu 4
7	MAN Truck & Bus AG Dachauer Str. 667 80995 München Nemecko	Všetky ostatné osobné údaje užívateľa, ktoré sa prenášajú príjemcovi zákazky prostredníctvom Connected Vehicle a/alebo Mobile Device	Hosting platformy
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Nemecko	Všetky ostatné osobné údaje užívateľov, ktoré sa prenášajú príjemcovi zákazky prostredníctvom vozidiel TBM1/2	Hosting platformy
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Švédsko	Všetky ostatné osobné údaje užívateľa, ktoré sa prenášajú prostredníctvom vozidla príjemcovi zákazky	Hosting platformy
10	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hannover Nemecko	Všetky ostatné osobné údaje užívateľa, ktoré sa prenášajú prostredníctvom vozidla príjemcovi zákazky	Hosting platformy

PRÍLOHA 2 – Technické a organizačné opatrenia
Technické a organizačné opatrenia príjemcu zákazky na zabezpečenie rizika v príslušnej úrovni ochrany, sú popísané v koncepte ochrany údajov k platforme RIO a predovšetkým zahŕňajú:

1. Pseudonymizáciu

Pokiaľ sa osobné údaje využívajú na účely vyhodnocovania, ktoré sú tiež vykonateľné so pseudonymizovanými údajmi, používajú sa techniky pseudonymizácie. Pritom sa najskôr vopred definuje pre každé pole údajov, či je potrebné pseudonymizovať, pretože by sa umožnil záver na osobu. Kľúče pseudonymizácie sa uložia do „Data Safe“, pre ktorý sa určí maximálne možné obmedzenie prístupu.

2. Šifrovanie

Mobilné koncové prístroje komunikujú šifrovane s koncovým bodom na základe individuálneho certifikátu na prístroje. Údaje sa ďalej šifrovane prenášajú v rámci platformy RIO („Ubiquitous encryption“ alebo „encryption everywhere“).

3. Zaručenie dôvernosti

Všetci zamestnanci budú poučení ohľadom dodržiavania povinnosti mlčanlivosti a písomne to musia aj potvrdiť.

Použitá IT infraštruktúra bude daná k dispozícii prostredníctvom Amazon Web Service (ďalej označované ako AWS) v rámci jedného cloudu (IaaS & PaaS) . Vstupnú kontrolu vykonáva poskytovateľ AWS Data - Center: vysoko zabezpečené výpočtové strediská AWS používajú elektronické kontrolné opatrenia ohľadom stavu techniky a viacstupňové systémy vstupnej kontroly. Výpočtové strediská disponujú 24 hodín denne vzdelaným bezpečnostným personálom a prístup je prísne zabezpečený podľa princípu najmenších práv a výhradne na účel systémovej administrácie.

Prístup ku komponentom hardware (clients) u TB Digital Services GmbH sa uskutočňuje podľa platných, individuálnych štandardných opatrení. Sú to napr. prístupové obmedzenia prostredníctvom rozjednocovacieho zariadenia (turniketu), videokamery, alarmu a/alebo strážnej služby, elektronických alebo mechanických bezpečnostných dverí, budov zabezpečených voči vlámaniu, zdokumentované oprávnenia na vstup (návštevy, cudzie sily) alebo deklarovanými bezpečnostnými oblasťami.

Vstupné kontroly zahŕňajú opatrenia na zabezpečenie prístrojov, siete a užívania.

Ako opatrenia na zabezpečenie prístrojov vo vozidle sa používajú rôzne opatrenia: Mobilné koncové zariadenia sú upevnené vo vozidle a disponujú secure boot, t. j. nie je tu možné stiahnuť cudzí prevádzkový systém a spustiť ho. Mobilné koncové prístroje komunikujú šifrovane s koncovým bodom na základe individuálneho certifikátu na prístroje. Údaje sa ďalej šifrovane prenášajú v rámci platformy RIO („Ubiquitous encryption alebo „encryption everywhere“). Koncové zariadenia pravidelným nahrávaním bezpečnostných supdates udržujú v aktuálnom bezpečnom stave (patch-management).

Ako opatrenia na zabezpečenie siete sa aplikujú tiež rôzne štandardné opatrenia: Sú implementované primerané (stavu techniky zodpovedajúce) údaje o heslách (dĺžka, komplexnosť, platnosť hesiel atď.). Opakované chybné zadanie identifikácie užívateľa/kombinácie hesla vedie k (dočasnému) zablokovaniu užívateľa. Sieť podniku je prostredníctvom firewall oddelená od nezabezpečených otvorených sietí. Proces je etablovaný, zabezpečuje pravidelné zásobovanie mobilnými prístrojmi s bezpečnostným supdates (proces OTA). Na odhalenie príp. zabránenie útokov na podnikovú sieť (intranet) sa využívajú vhodné technológie (napr. intrusion detection systeme). Zamestnanci sa pravidelne senzibilizujú proti nebezpečenstvám a rizikám.

Ako opatrenia na zabezpečenie užívania sa aplikujú niektoré štandardné opatrenia:

Relevantné užívanie je zabezpečené prostredníctvom primeraných mechanizmov autentizácie a autorizácie voči nepovolenému vstupu. Sú implementované primerané (stavu techniky zodpovedajúce) údaje o heslách (dĺžka, komplexnosť, platnosť hesiel atď.). Pre použitie s osobitnou ochranou sa používajú silné autentizačné mechanizmy (napr. Token, PKI). Opakované chybné zadanie identifikácie užívateľa/kombinácie hesla vedie k (dočasnému) zablokovaniu užívateľa. Údaje použité v relevantnom procesu sa nachádzajú v zašifrovanej forme na mobilnom nosiči údajov. Zrealizované prístupy a pokusy o prístup sa protokolujú. Vytvorené protokolové súbory sa na určitý čas (min. 90 dní) ukladajú a (námatkovo) kontrolujú.

Oprávnenia užívateľa (pre prístup) sú zabezpečené rôznymi opatreniami, pričom tieto sú zásadne pridelené určitej osobe. Oprávnenia udeľujú zodpovední za platformu a pravidelne sa kontrolujú. Udelenie oprávnenia k prístupu sa uskutočňuje len na základe definovaného a zdokumentovaného procesu. Zmena oprávnení na prístup sa uskutočňuje podľa princípu štyroch očí a zdokumentujú sa vo verziovej logfile.

Ako opatrenia na kontrolu prístupu príp. riadenia sa aplikujú rôzne opatrenia: Prístupové práva sa definujú a zdokumentujú v rámci konceptu oprávnení / rolí a sú usporiadané podľa požiadaviek na základe úloh súčasných rolí. Sú zriadené špecifické role/oprávnenia pre technickým administrátorov (ktorí, pokiaľ je to technicky možné, neumožňujú prístup k osobných údajom). Sú zriadené špecifické role/oprávnenia pre odborný support (ktoré neobsahujú žiadne technické administratívne práva).

Definícia rolí/oprávnení a priradenie rolí/oprávnení sa uskutoční, pokiaľ je to technicky a organizačne možné, nie prostredníctvom tej istej osoby, v jednom bezpečnom revíznom (povoľovacom-) konaní a je časovo obmedzená. Priame prístupy do databázy pri obídení konceptu rolí/oprávnení sú možné len prostredníctvom autorizovaných administrátoroch databázy. Existuje úprava pre aplikáciu súkromného nosiča údajov príp. použitie súkromného nosiča údajov je zakázané. Existujú záväzné predpisy ohľadom prístupov do údajov pri externej údržbe, diaľkovej údržbe a práce na diaľku. Na základe práva na ochranu údajov sa uskutočňuje ničenie/ likvidácia dokumentov a nosičov údajov (napr. Schredder, tona na ochranu údajov) prostredníctvom spoľahlivých podnikov na likvidáciu.

Koncept rolí a oprávnení sa pravidelne prispôsobuje meniacim sa pracovným organizačným štruktúram (napr. nové role) a priradené role/oprávnenia sa pravidelne kontrolujú (napr. prostredníctvom nadriadených) a poprípade sa prispôsobujú, príp. odnímajú. Vykonáva sa pravidelná centrálne kontrola príp. pridelený

štandardný profil. Meniace sa prístupy (zápis, vymazávanie) sa zaprotokolujú a vytvorené súbory protokolov sa na určitý čas (min. 90 dní) ukladajú a (námatkovo) kontrolujú.

Ako všeobecné opatrenia na zabezpečenie postúpenia sa aplikujú rôzne štandardné opatrenia:

Osoby poverené postúpením sa vopred zoznámia s bezpečnostnými opatreniami. Vopred sa stanoví okruh prijímateľov tak, že sa zabezpečí zodpovedajúca kontrola (autentizácia). Je stanovený a zdokumentovaný celý proces prenosu údajov a vykonanie konkrétneho prenosu údajov sa zaprotokoluje, príp. zdokumentuje (napr. potvrdenie o príjme, príjmový doklad). Osoby poverené na prenos vykonajú vopred kontrolu hodnovernosti, kompletnosti a správnosti.

Pred vykonaním konkrétneho prenosu údajov sa uskutoční kontrola adresy prijímateľa (napr. e-mail adresy). Prenos údajov internetom sa realizuje v zašifrovanej forme (napr. zašifrovanie súboru). Integrita prenášaných dát, pokiaľ je to technicky možné, sa zabezpečuje prostredníctvom aplikácie podpisového procesu (digitale signatur). Elektronické potvrdenie prijatie sa vo vhodnej forme archivuje. Neželanému prenosu údajov internetom sa zabráni vhodnými technológiami (napr. proxy, firewall).

Ďalej sa ako opatrenia na vykonanie oddeleného príkazu uplatnia nasledujúce štandardné opatrenia:

Existujú záväzné predpisy ohľadom účelovej väzby spracovania na dodržanie oddeleného príkazu. Údaje stanovené k určitému účelu sa oddelia od ostatných údajov a podľa toho sa uložia. Aplikované IT systémy umožňujú oddelené ukladanie údajov (prostredníctvom mandátu alebo prístupových konceptov). Uskutoční sa oddelenie údajov v testovacích a produktívnych systémoch. U pseudonymizovaných údajoch sa oddelene uloží kľúčový most, ktorý umožňuje opätovnú identifikáciu údajov. Pri spracovaní zákazky alebo prenose funkcie sa uskutoční oddelené spracovanie údajov rôznych zadávateľov zákazky u príjemcu zákazky. Existujúce koncepty rolí/oprávnení umožňujú prostredníctvom ich usporiadania logické rozdelenie spracovaných údajov.

4. Zabezpečenie integrity

Ako opatrenia na vykonanie protokolu vstupných údajov sa používajú rôzne štandardné opatrenia:

Zaprotokolujú sa prístupové práva ako aj všetky činnosti administrátora. Zaprotokolujú sa prístupy (vstupy, zmeny, zmazania) a zmeny na údajových poliach (napr. obsah nového alebo zmeneného súboru dát). Nasleduje zaprotokolovanie prenosov (napr. download) a Login - zaprotokolovanie.

Z dôvodu prehľadnosti údajov sa použité záznamy zdokumentujú a archivujú. U protokolu sa uvádza dátum a čas, užívateľ, druh aktivity, užívateľský program a poradové číslo záznamu. Zdokumentujú sa nastavenia protokolu.

Zaručuje sa výlučne jeden prístup do súborov protokolov. Okruh oprávnených osôb na prístup do protokolových súborov je pevne ohraničený (napr. pre administrátorov,osôb poverených na ochranu údajov, revízorov). Protokolové súbory sa archivujú na určité obdobie (napr. 1 rok) a potom sa na základe práva na ochranu údajov

vymažú. Protokolové súbory sa pravidelne automatizovane vyhodnocujú. Vyhodnotenia protokolových súborov sa vyhotovujú, pokiaľ je to možné, v pseudonymizovanej podobe.

5. Zabezpečenie dostupnosti

Architektúra je zabezpečená prostredníctvom interných mechanizmov replikácie v rámci platformy AWS per se voči strate údajov. Ďalej sa ako opatrenia na zabezpečenie objektu aplikujú nasledujúce štandardné opatrenia AWS:

Vykonajú sa protipožiarne opatrenia (napr. protipožiarne bezpečnostné dvere, hlásič dymu, protipožiarne steny, zákaz fajčenia). Počítače sú chránené pred povodňami (napr. počítačová miestnosť sa nachádza na 1. poschodí, hlásič vody). Vykonávajú sa opatrenia proti otrasom (napr. počítačová miestnosť nie je v blízkosti diaľníc, železničných koľajníc, strojových miestností). Počítače sú chránené proti elektromagnetickým poliam (napr. oceľové platne vo vonkajších stenách). Vykonávajú sa opatrenia voči vandalizmu a krádeži (porovnaj vstupnú kontrolu). Počítače sa nachádzajú v klimatizovaných priestoroch (teplota a vlhkosť vzduchu sú regulované klímou). Počítače sú zaistené prepäťovou ochranou proti prepäťovým hrotom. Vykonávajú sa opatrenia na zabezpečenie nízkoprúdového a kontinuálneho zásobovania prúdom (napr. prístroje USV, núdzové napájacie agregáty).

Súbory údajov sa pravidelne zabezpečujú vo forme back up kópii v rámci platformy AWS. Backup Koncept sa dokumentuje a pravidelne kontroluje a aktualizuje. Backup Média sú chránené pred nepovoleným vstupom. Použité backup programy zodpovedajú aktuálnym štandardom kvality a pravidelne sa aktualizujú. Zriaďuje sa redundantné výpočtové stredisko (vzdialené od miesta spracovania) a v prípade katastrofy je schopné pokračovať v spracovaní údajov. V pláne núdzového manažmentu AWS sa zdokumentujú rôzne opatrenia na kontrolu dostupnosti.

Predtým ako je zákazka odovzdaná na spracovanie, príjemca zákazky starostlivo skontroluje podľa stanovených kritérií (technické a organizačné opatrenia). K tomu sa vyžaduje detailný výklad technických/organizačných opatrení na ochranu údajov vedený príjemcom zákazky (odpovede na súbor otázok alebo koncept na ochranu údajov) a následná kontrola. V závislosti od množstva a citlivosti spracovaných údajov sa uskutoční kontrola príp. tiež miestna kontrola u príjemcu zákazky. Pri výbere príjemcu zákazky sa zohľadňujú vhodné certifikácie (napr. ISO 27001). V primeranej a prijateľnej forme sa zdokumentujú zistené kvalifikácie príjemcu zákazky.

Na vytvorenie zmluvného vzťahu sa uzatvorí zmluva o spracovaní osobných údajov medzi zadávateľom zákazky a príjemcom zákazky. Ten určí detailne a písomne oprávnenosti a zodpovednosti ako aj povinnosti obidvoch zmluvných strán. Pokiaľ poverený poskytovateľ služieb má sídlo mimo EÚ príp. EHP, použijú sa klauzuly štandardnej zmluvy EÚ. Je zmluvne stanovené, že spracovanie údajov príjemcom zákazky sa smie uskutočniť len v rámci pokynov zadávateľa zákazky. Príjemca zákazky je povinný, bezodkladne poučiť zadávateľa zákazky o tom, ak niektorý z pokynov, podľa mienky príjemcu zákazky, poruší predpisy na ochranu údajov. Z dôvodu ochrany práv dotknutých osôb sa v zmluve na spracovanie osobných údajov dohodne, aby príjemca zákazky

primerane podporoval zadávateľa zákazky, pokiaľ je toto požadované napr. v prípade podávania informácií dotknutým osobám.

V ďalšom priebehu spracovania osobných údajov zadávateľ kontroluje pracovné výsledky príjemcu zákazky so zreteľom na formu a obsah údajov. Pravidelne sa kontroluje dodržiavanie technických a organizačných opatrení u príjemcu zákazky. K tomu sa prevažne používa predloha aktuálnych osvedčení alebo vhodných certifikácii príp. doklad o vykonaných auditoch IT bezpečnosti alebo ochrany údajov. Pokiaľ sa použije subdodávateľ, zmluvne sa stanoví, že tieto sa zodpovedajúco skontrolujú.

6. Zabezpečenie zaťažiteľnosti systémov

Ako jedna z najflexibilnejších a najbezpečnejších okolí cloud computing sa vytvorila infraštruktúra AWS cloud. Tá bola koncipovaná ako optimum dostupnosti pri plnom oddelení zákazníkov. Dodáva extrémne stupňovitú rozšíriteľnú, veľmi bezpečnú prevádzkovú platformu, ktorá dovoľuje zákazníkom, preniesť obsahy, v prípade potreby, rýchlo a bezpečne do celého sveta. Služby AWS sú potiaľ nezávislé od obsahu, pokiaľ poskytujú všetkým zákazníkom rovnakú úroveň bezpečnosti, nezávisle od druhu obsahov alebo geografického regiónu, v ktorom sú obsahy uložené.

Vysoko zabezpečené výpočtové centrá AWS na úrovni svetových tried používajú elektronické kontrolné opatrenia na kontrolu stavu techniky a viacstupňové systémy vstupných kontrol. Výpočtové strediská disponujú 24 hodín denne vzdelaným bezpečnostným personálom a prístup je prísne zabezpečený podľa princípu najmenších práv a výhradne na účel systémovej administrácie.

7. Proces na obnovu dostupnosti osobných údajov podľa fyzického alebo technického incidentu.

Výpočtové strediská AWS sú zriadené v clusternoch v rôznych regiónoch sveta. Všetky výpočtové strediská sú online a obsluhujú zákazníkov; žiadne výpočtové stredisko nie je vypnuté. Pri výpadku posunú automatické procesy prenos údajov o zákazníkoch z dotknutých oblastí. Základné použitia sa zabezpečia v konfigurácii N+1 tak, že v prípade výpadku výpočtového strediska bude k dispozícii dostatok kapacity, aby sa prenos údajov rozdelil na zostávajúce stanoviská.

AWS ponúka flexibilitu, inštanciu a archivuje údaje v rámci viacerých geografických regiónov ako aj cez viaceré zóny availability v rámci jednotlivých regiónov. Každá zóna availability sa vyvíjala nezávisle od výpadkovej zóny. To znamená, že zóny availability sú v rámci typického mestského regiónu fyzicky rozdelené a nachádzajú sa napr. v oblastiach s nízkym rizikom povodní (podľa regiónu existujú rôzne kategorizácie povodňových zón). Dodatočne k samostatnému, neprerušovanému zásobovaniu elektrickou energiou a miestnymi generátormi na núdzový prúd sa napájajú všetky zóny availability cez rôzne siete prúdu od nezávislých zásobovateľov elektrickým prúdom, aby sa minimalizovali miesta chýb. Všetky zóny dostupnosti sú bezpečne prepojené s viacerými Tier-1-Transit-Providern.

Amazon tím na spravovanie incidentov používa v brandži obvyklé diagnostické procesy, na zrýchlenie odstránenia incidentov, ktoré sú kritické pre podnikanie. Prevádzkový personál je neustále k dispozícii 24 hodín denne sedem dní v týždni a 365 dní v roku, aby sa rozpoznali rušivé vplyvy a ich pôsobenie a odstránenie.

8. Pravidelná kontrola, vyhodnocovanie a hodnotenie účinnosti technických a organizačných opatrení.

So zreteľom na zavedenie a prevádzku platformy RIO sa zavádzajú smernice a pokyny, príp. implementované štandardy na zabezpečenie informácií, ktoré sa v podniku využívajú. K dispozícii sú prevádzkové funkcie na ochranu údajov a zabezpečenie informácii (osoba poverená na ochranu údajov a Information Security Officer). Zamestnanci sú povinní dodržiavať mlčanlivosť o údajoch a informovať o opatreniach na zabezpečenie údajov príp. IT bezpečnosti prostredníctvom brožúr, flyer, intranetových pokynov atď.

Skontrolujú sa Interné procesy so zameraním na dodržiavanie technických a organizačných opatrení, na zabezpečenie údajov prostredníctvom revízie, zabezpečenia informácii a ochrany údajov.

Procesy spracovania a opatrenia na zabezpečenie údajov sa zdokumentujú v zozname spracovateľských činností. Pravidelne sa koná kontrola (interná a externá) so zameraním na účinnosť opatrení.