Smlouva o zpracování objednávky (podle čl. 28 GDPR)

mezi

uživatelem (jak je stanoveno v hlavní smlouvě)

(dále jako „**Objednatel**“)

a

společností **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 Mnichov

(dále jako „**Dodavatel**“)
(Objednatel a Dodavatel dále jako „**Strana**“ a společně jako „**Strany**“).

Předmluva

(A) Tato smlouva o zpracovávání objednávky (dále jako „**Smlouva**“) se vztahuje na všechny činnosti, u kterých dodavatel přijde do styku s osobními daty objednatele (jak je určeno v článku 1.5 dole), od třetího poskytovatele nebo jiné dotčené osoby v souvislosti s činností popsanou v článku 2 všeobecných rámcových podmínek pro využívání platformy a případně k tomu uzavřených jednotlivých smluv pro další služby (dále jako „**Hlavní smlouva**“).

(B) V rámci této smlouvy jedná objednatel jako odpovědná osoba a dodavatel jako zpracovatel objednávky v rámci zpracovávání objednávky dle § 28 GDPR (jak je stanoveno níže).

Strany se proto dohodly následovně:

1 Definice a interpretace

1.1 „**Evropské právo**“ je platné právo Evropské unie, platné zákony současných členských států Evropské unie a platné zákony každého státu, který se následně stane členským státem Evropské unie.

1.2 „**Evropské právo o ochraně osobních dat**“ je platné právo Evropské unie o zpracovávání osobních dat (především DS-GVO), platné zákony současných členských států Evropské unie o zpracovávání osobních dat (především BDSG v aktuálním platném znění) a platné zákony každého státu, který se následně stane členským státem Evropské unie, o zpracovávání osobních dat.

1.3 „**DS-GVO**“ je „NAŘÍZENÍ (EU) 2016/679 EVROPSKÉHO PARLAMENTU A RADY z 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)“.

1.4 „**BDSG**“ je Spolkový zákon o ochraně dat.

1.5 „**Osobní data**“ mají význam, jak je definováno v BDSG/ v DS-GVO.

2 Předmět zpracování údajů / Povinnosti objednatele

2.1 Tato smlouva upravuje povinnosti stran v souvislosti se zpracováváním osobních dat objednatele dodavatelem v rámci hlavní smlouvy uvedené v Příloze 1.

2.2 Předmět a trvání zpracovávání, druh a účel zpracovávání, druh osobních dat, kategorie dotčených osob a povinnosti a práva odpovědných osob vyplývají z Přílohy 1 této smlouvy a zadávací specifikace hlavní smlouvy.

2.3 Objednatel zůstává odpovědnou osobou ve smyslu GDPR a zaručuje spolehlivost zpracování osobních údajů o příslušných osobách (řidič a případně další osoby). V tomto ohledu bude objednatel dodržovat zejména svou rozsáhlou informační povinnost a zajistí, aby byl pro zpracování osobních údajů k dispozici právní důvod pro ochranu údajů (např. uzavření podnikové dohody, omezení zpracování pro účely zaměstnaneckého poměru).

3 Povinnosti Dodavatele

3.1 Dodavatel bude zpracovávat osobní data objednatele výlučně pro účely uvedené v Příloze 1 a v rámci hlavní smlouvy a v objednávce a dle zdokumentovaných pokynů objednatele v Příloze 1; dodavatel nebude zpracovávat osobní data v rámci této smlouvy k jiným účelům. Tímto nedotčeno zůstává zpracovávání mimo rámec této smlouvy pro vlastní účely dle článku 8.3.4 hlavní smlouvy. Kopie nebo duplikáty osobních dat nebudou bez vědomí objednatele pořizovány. Výjimkou jsou záložní kopie, pokud jsou potřebné pro záruční plnění řádného zpracovávání dat, a data potřebná s ohledem na dodržení zákonné povinnosti jejich ukládání.

3.2 Po ukončení poskytování zpracovatelských služeb musí dodavatel veškerá osobní data objednatele objednateli dle jeho volby vydat a/nebo řádně dle zákona o ochraně dat smazat, pokud tomu nebudou bránit zákonné lhůty archivace dat dle práva a pokud je dodavatel nezpracovává pro vlastní účely mimo rámec této smlouvy dle článku 8.3.4 hlavní smlouvy. Totéž platí pro zkušební a odpadový materiál. Úplné smazání nebo vydání dat Objednateli mu musí být na vyžádání písemně potvrzeno s uvedením data.

3.3 Pokud je to zahrnuto v rozsahu plnění, podpoří dodavatel objednatele při plnění práv dotčené osoby (informace, opravení, námitka, vymazání) podle příslušného pokynu objednatele.

3.4 Dodavatel potvrzuje, že – pokud to zákon vyžaduje – pověří osobu odpovědnou za ochranu dat v podniku (srov. § 38 BDSG/čl. 37 GDPR).

3.5 Dodavatel je povinen objednateli ihned sdělit výsledek kontrol úřadů pro kontrolu ochrany dat, pokud to souvisí se zpracováváním dat Objednatele. Zjištěné nedostatky budou Dodavatelem během přiměřené doby odstraněny a sděleny Objednateli.

3.6 Zpracovávání dat Dodavatelem a subdodavateli schválenými Objednatelem bude probíhat výlučně na území Spolkové republiky Německo, v členském státě Evropské unie nebo jiném dohodnutém státě Evropského hospodářského prostoru. Každé přesunutí do jiné země (dále jako „**Třetí země**“) vyžaduje předchozí výslovný souhlas objednatele a navíc smí proběhnout pouze tehdy, pokud jsou splněny zvláštní předpoklady pro export dat do třetích zemí (srov. čl. 40 ff. GDPR). K tomu je případně nutné přiložit údaje uvedené v Příloze 1 a další (smluvní) podklady.

3.7 Dodavatel musí zaměstnance pověřené prováděním prací seznámit s důležitými ustanoveními o ochraně dat a ti se musí zavázat k zachovávání mlčenlivosti (srov. čl. 28 GDPR odst. 3 b)) a vhodnými kroky zajistit, aby tito zaměstnanci zpracovávali osobní údaj pouze na pokyn objednatele.

3.8 Dodavatel pravidelně kontroluje dodržování předpisů o ochraně dat dle této smlouvy a dokumentuje pokyny Objednatele během celé doby platnosti Smlouvy. Výsledky kontrol budou Objednateli na vyžádání předloženy, pokud jsou pro zpracovávání dat Objednatele relevantní. Opatření na kontrolu jsou popsány v koncepci ochrany dat, která se musí předložit Objednateli.

3.9 Dodavatel musí Objednateli poskytnout vzhledem k povaze zpracovávání a dle možností součinnost vhodnými technickými a organizačními opatřeními pro splnění povinnosti respektovat práva dotčených osob uvedené v kapitole III DS-GVO. Dodavatel při tom nese Objednateli tím vzniklé náklady.

3.10 Dodavatel musí Objednateli vzhledem ke způsobu zpracování a jemu poskytovaných informaci při dodržování povinnosti dle čl. 32 až 36 DS-GVO poskytnout součinnost.

4 Technická a organizační opatření pro bezpečnost dat

4.1 Dodavatel provede přiměřená technická a organizační opatření na ochranu dat (srov. čl. 32 GDPR). Dodavatel je především povinen provést technická a organizační opatření smluvně dohodnutá v příloze 2 k této smlouvě. Tato opatření Dodavatel přizpůsobí vzhledem k obchodnímu vztahu technickým a organizačním podmínkám, aniž by se tím snížila úroveň ochrany. Důležité změny musí být dohodnuty písemně.

4.2 Dodavatel prokáže Objednateli na vyžádání skutečné dodržení technických a organizačních opatření.

4.3 Dodavatel je povinen vést přiměřenou dokumentaci pro zpracovávání dat, na základě které bude moci Objednateli předložit doklad o řádném zpracovávání dat. Doklad může proběhnout i formou schválené certifikace dle čl. 42 DS-GVO.

5 Subdodavatelé

5.1 Dodavateli je tímto dovoleno ustanovovat Subdodavatele uvedené v Příloze 1.

5.2 Využívání dalších subdodavatelů se tímto povoluje. Dodavatel bude Objednatele informovat o každé plánované změně týkající se přidávání nebo změny subdodavatelů; Objednatel může vznést proti plánované změně výhradu. Nesubdodavatelské vztahy jsou ve smyslu tohoto ustanovení takové služby, které Dodavatel uplatní u Třetích osob jako vedlejší dodávku, jako pomoc s plněním objednávky. Tím se myslí například telekomunikační služby, úklidové služby, kontroly nebo likvidace datových nosičů. Dodavatel je ale povinen pro záruční plnění ochrany a bezpečnosti dat Objednatele i u vedlejších plnění zadaných externě uzavírat přiměřené a zákonné smluvní dohody a provádět kontroly.

5.3 Využije-li dodavatel služeb subdodavatele, musí dodavatel zajistit, aby mu byly formou (i) smlouvy uzavřené mezi subdodavatelem a dodavatelem nebo (ii) dalšího právního nástroje dle evropského práva na ochranu dat uloženy stejné povinnosti na ochranu dat, jako byly uloženy dodavateli dle této smlouvy. Při tom musí dodavatel především zaručit, aby byla prováděna vhodná technická a organizační opatření tak, že proběhne zpracování osobních dat v souladu s požadavky GDPR. Na písemnou žádost Objednatele Dodavatel Objednateli sdělí hlavní obsah smlouvy a uplatnění povinnosti na ochranu osobních dat ve vztahu se Subdodavatelem, popřípadě mu umožní nahlédnout do relevantních podkladů smlouvy. Komerční podmínky při tom Dodavatel nesmí začernit. Objednatel se zavazuje zachovávat mlčenlivost o získaných informacích.

6 Práva kontroly

6.1 Objednatel má právo kontrolovat dodržování povinností z této smlouvy (včetně udělených pokynů) sám nebo je nechat zkontrolovat jím pověřenou třetí osobou.

6.2 Dodavatel poskytne Objednateli při kontrolách přiměřenou součinnost. Dodavatel objednateli především umožní přístup k zařízením na zpracovávání dat a poskytne mu potřebné informace.

6.3 Pro případ, že by bylo výsledkem kontroly to, že dodavatel a/nebo zpracovávání nesplňuje požadavky dle této smlouvy a/nebo Evropského zákona na ochranu osobních dat, musí Dodavatel provést veškerá opatření na nápravu, která jsou nutná, aby zajistil dodržování ustanovení tohoto zákona a/nebo Evropského zákona o ochraně dat.

6.4 Náklady, které objednateli vzniknou prováděním kontroly, nese on sám. Náklady, které dodavateli vzniknou prováděním kontroly ze strany Objednatele, může požadovat po Objednateli, pokud Objednatel kontrolu provádí nebo nechává provádět častěji než jedenkrát v kalendářním roce.

6.5 Kontroly u Dodavatele budou včas oznámeny a nesmí neúměrně omezit provoz Dodavatele.

7 Povinnost informovat

Dodavatel bude Objednatele ihned informovat, pokud by pokyn udělený Objednatelem dle mínění dodavatele porušoval Evropský zákon o ochraně dat. Pokyn, který by znamenal porušení práva, nemusí být vykonán, dokud nebude Objednatelem změněn nebo výslovně potvrzen. Materiálně právní kontrola pokynů není povinností Dodavatele.

Dodavatel při zjištění chyb nebo odchylek ve zpracování dat nebo při podezření na porušení ochrany dat (společně dále jako „**Případ**“) o tom bude neprodleně objednatele informovat. Dodavatel musí případ zdokumentovat i se všemi věcnými okolnostmi, důsledky a všemi opatřeními na jeho odstranění a na žádost objednatele tyto zdokumentované informace ihned písemně nebo elektronicky předat objednateli.

8 Odpovědnost a výjimky

8.1 Dodavatel ručí za škody, které způsobí on nebo je způsobí jeho pomocníci v plnění úmyslně a/nebo hrubou nedbalostí. Za škody způsobené nedbalostí Dodavatele nebo jeho pomocníků v plnění, odpovídá Dodavatel pouze, pokud byla porušena kardinální povinnost. Kardinálními povinnostmi jsou důležité povinnosti, které umožňují řádnou proveditelnost smlouvy, a na jejichž plnění Objednatel spoléhal a směl spoléhat. Při nedbalosti týkající se porušení těchto kardinálních povinností je odpovědnost Dodavatele omezena na běžně předvídatelné škody.

8.2 Objednatel zbavuje Dodavatele odpovědnosti za veškeré nároky třetích osob (včetně dotčených osob a/nebo úřadů ochrany dat), škody a náklady, které vzniknou porušením ustanovení této smlouvy a/nebo Evropského práva o ochraně dat ze strany Objednatele; to neplatí, pokud Objednatel chybu nezavinil a pokud Dodavatel k chybě přispěl.

9 Doba platnosti

Doba platnosti smlouvy odpovídá době platnosti Hlavní smlouvy. Ukončením Hlavní smlouvy z jakékoli důvodu končí automaticky i platnost této smlouvy. Právo na vypovězení smlouvy z váženého důvodu tímto zůstává nedotčeno.

10 Ostatní

10.1 Plnění Dodavatele dle této smlouvy budou zaplacena dle ustanovení o úhradě upraveného v hlavní smlouvě.

10.2 Jsou-li osobní data objednatele u dodavatele opatřeními třetích osob (cca zástavou nebo zabavením) v důsledku insolvence nebo insolvenčního řízení či jinými podobnými opatřeními ohrožena, musí o tom dodavatel objednatele ihned informovat.

10.3 Budou-li jednotlivá ustanovení této Smlouvy neúčinná nebo se stanou neúčinnými, zůstává tím účinnost zbylých ustanovení nedotčena. Strany se v případě neúčinnosti ustanovení dohodnou na novém ustanovení, které se bude co nejvíce blížit věcnému a hospodářskému účelu smlouvy.

10.4 V případě, že dojde k vystoupení Velké Británie z Evropské unie, je Dodavatel povinen již k uzavření všech dohod a provedení všech kroků, které jsou nutné, aby bylo zpracovávání dat dle smlouvy ve Velké Británii od okamžiku vystoupení u Evropské unie přípustné. Pokud k okamžiku vystoupení nebude k dispozici žádné pozitivní rozhodnutí evropské komise o přiměřenosti, jsou to z dnešního pohledu především standardní ustanovení o ochraně dat dle článku 46 odst. 2 c) pro poskytování osobních dat zpracovatelům objednávek, kteří mají zastoupení v třetích zemích, v nichž není zajištěna přiměřená úroveň ochrany.

Pokud dodavatel tyto povinnosti nesplní, je objednatel oprávněn požadovat po dodavateli s účinností od vystoupení Velké Británie z Evropské unie, aby příslušná plnění vykonával firmou, nebo částí firmy se stálým sídlem na území Evropské unie, aniž by tím objednateli vznikly vícenáklady nebo další náklady.

10.5 Tato smlouva o zpracování objednávky je k dispozici v 18 jazykových verzích, přičemž v případě odchylek má přednost originální znění.

10.6 Tato smlouva se řídí Právem Spolkové republiky Německo s vyloučením Úmluvy OSN o kontraktech na mezinárodní prodej zboží. Místně příslušný soud je výlučně v Mnichově.

10.7 Následující přílohy jsou součástí smlouvy:

Příloha 1 – Popis zpracovávání objednávky
Příloha 2 – Technická a organizační opatření

PŘÍLOHA 1 – Popis zpracovávání objednávky

1 Hlavní smlouva

Hlavní smlouva ve smyslu článku 2.1 hlavní části smlouvy jsou „Všeobecné rámcové podmínky pro využívání platformy“.

Titul/Strany: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 Mnichov / **Uživatel**

2 Předmět a trvání objednávky

Předmět objednávky vyplývá z článku 1 (*Předmět*) a článku 8 (*Data Uživatele a ochrana dat*) hlavní smlouvy; trvání objednávky vyplývá z článku 7 (*Uzavření smlouvy, doba trvání smlouvy a práva na vypovězení smlouvy*) hlavní smlouvy.

3 Rozsah, druh a účel zpracování dat / opatření při zpracovávání dat

Rozsah, druh a účel zpracování osobních dat vyplývají z článku 8 hlavní smlouvy.

Bližší popis předmětu objednávky s ohledem na rozsah, druh a účel:

Pro poskytování dodavatelem nabízených služeb (jak je definováno v Hlavní smlouvě), musí dodavatel zjišťovat osobní data objednatele přes Connected Vehicles nebo Mobile Devices (a případně také osobní data poskytovaná třetím poskytovatelem, s kterým se uživatel dohodne na užívání zprostředkovaných služeb) v míře potřebné pro zajišťování jím poskytovaných služeb, přenášet je na platformu a zde ukládat. Dodavatel bude zpracovávat data ukládaná na platformu v rozsahu nutném pro poskytování služeb (k přibližné analýze jízdních vlastností řidiče a používání Connected Vehicle nebo Mobile Device na základě osobních dat a vyhodnocovat je a poskytovat objednateli na tomto základě nabídky, jako jsou tréninkové programy pro řidiče, výbava a návrhy na zvýšení efektivity). Přesný rozsah, druh a účel vyplynou především z dodatečně uzavíraných individuálních smluv.

4 Okruh dotčených osob (kategorie dotčených osob)

Zpracováváním objednávky jsou dotčeny následující okruhy osob:

- **Řidiči a další zaměstnanci**(zaměstnanci vlastní společnosti objednatele), např. zaměstnanci, učni, uchazeči, bývalí zaměstnanci*;*
- **Řidiči**, kteří nejsou zaměstnanci;
- **Kontaktní osoba** personálu pro nakládku/vykládku a jiní obchodní partneři objednatele; a
- **Pracovníci koncernu** (pracovníci jiné společnosti skupiny Objednatele).

5 Druh osobních dat

Zpracovávání objednávky zahrnuje následující druhy osobních dat:

- Jméno řidiče a identifikační číslo řidiče;
- Identifikační číslo vozidla;
- Data o stanovišti;
- Data týkající se doby řízení a přestávek;
- Data týkající se chování při jízdě;
- Stavová data Connected Vehicle;
- Stavová data traileru;
- Stavová data návěsů nástaveb, agregátů a dalších částí vozidla;
- Stavová data případných připojených IOT Devices
- Stavová data Mobile Devices;
- Data týkající se naložení;
- Data objednávky; a
- Kontaktní data kontaktních osob pro nakládku/vykládku a jiní obchodní partneři Objednatele.

6 Zdokumentované pověření

Objednatel tímto pověřuje dodavatele zpracovávání osobních dat, jak je uvedeno v článku 8 hlavní smlouvy. To zahrnuje především následující zpracování:

- Osobní data jsou přenášena přes Connected Vehicle nebo Mobile Device na cloudovou platformu dodavatele a zde ukládána.
- Osobní data jsou dle této smlouvy zpracovávána pouze, pokud je to nutné ke splnění hlavní smlouvy; článek 8.3.4 hlavní smlouvy tímto zůstává nedotčen.
- Dodavatel předá osobní data třetímu poskytovateli (jak je určeno v hlavní smlouvě), pokud a nakolik je takové poskytnutí třetímu poskytovateli nutné, aby mohl objednateli poskytovat své zprostředkované služby (jak je určeno v hlavní smlouvě).
- Dodavatel bude na základě osobních dat analyzovat jízdní vlastnosti řidiče a používání Connected Vehicle vyhodnocovat a poskytovat objednateli na tomto základě pro jeho potřeby na míru ušitě nabídky, jako jsou tréninkové programy pro řidiče, výbava a návrhy na zvýšení efektivity.

7 Místo zpracování

- Německo.
- Spojené království; pokud data pro účely IT hostingu a/nebo IT podpory budou zpracovávána v rámci Evropské unie, budou uzavřeny příslušné smlouvy o zpracovávání dat objednávek.

- Pokud bude dodavatel pro účely IT hostingu a/nebo IT podpory využívat subdodavatele mimo území Evropské unie (k tomu viz článek 8 této přílohy 1), proběhne předání osobních dat na základě standardní smluvních klauzulí/standardních klauzulí o ochraně osobních dat uzavřené mezi dodavatelem a subdodavatelem o zaslání osobních údajů zpracovatelem objednávky do třetích států podle čl. 46 odst. 2 c) GDPR.

8 Subdodavatelé

Dodavatel ustanovuje následující subdodavatele (kteří mohou případě ustanovit další subdodavatele):

Č.	Subdodavatel (firma, adresa, kontaktní osoba)	Zpracované kategorie dat	Kroky zpracování / účel zpracování subdodávky
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Veškerá osobní data platformy související s částí prodeje (tzn., kde se může zákazník na platformu zaregistrovat a provádět objednávky)	Hosting platformy
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Veškerá osobní data platformy související s částí prodeje (tzn., kde se může zákazník na platformu zaregistrovat a provádět objednávky)	IT podpora týkající se platformy
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 USA https://aws.amazon.com/de/compliance/contact/	Veškerá další osobní uživatelská data poskytovaná přes vozidlo dodavateli	Hosting platformy / IT podpora pro hosting platformy
4	Rovněž budoucí místo 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/	Veškerá další osobní uživatelská data poskytovaná přes vozidlo dodavateli	Hosting platformy
5	MAN Service und Support GmbH Dachauer Straße 667 80995 Mnichov Německo	Veškerá osobní data pro zpracovávání požadavků zákazníků potřebná v rámci 1. a 2. úrovně podpory	1. úroveň podpory

6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 USA	Veškerá osobní data potřebná pro zpracovávání faktur/objednávek	Hosting platformy (EU Tenant – Gehosted by Amazon Web Services (EU) – viz čl. 4
7	MAN Truck & Bus AG Dachauer Str. 667 80995 Mnichov Německo	Veškerá další osobní uživatelská data poskytovaná dodavateli přes Connected Vehicle a/nebo Mobile Device	Hosting platformy
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Německo	Veškerá další osobní uživatelská data poskytovaná dodavateli přes vozidla TBM1/2	Hosting platformy
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Švédsko	Veškerá další osobní uživatelská data poskytovaná přes vozidlo dodavateli	Hosting platformy
10	Volkswagen Nutzfahrzeuge (užitná vozidla) Mecklenheidestr. 74 30419 Hannover Německo	Veškerá další osobní uživatelská data poskytovaná přes vozidlo dodavateli	Hosting platformy

PŘÍLOHA 2 - Technická a organizační opatření
Technická a organizační opatření prováděná Dodavatelem pro zajištění dle rizika přiměřené úrovně ochrany, jsou popsána v koncepci ochrany dat pro platformu RIO a zahrnují především:

1. Pseudonymizace

Pokud jsou osobní data využívána pro účely vyhodnocování, proveditelné i s pseudonymizovanými daty, bude používána pseudonymizace. Při tom se nejprve pro každé datové pole definuje, zda musí být pseudonymizováno, protože by bylo možné zpětně vyvodit určitou osobu. Kódy pro pseudonymizaci jsou ukládány v „Data Safe“, aby bylo dosaženo maximálního možného omezení přístupu.

2. Kódování

Mobilní koncová zařízení komunikují s koncovým bodem kódovaně na základě individuálního certifikátu zařízení. Data jsou v rámci platformy RIO dále předávána kódovaná („Ubiquitous encryption“ nebo „encryption everywhere“).

3. Zajištění důvěrnosti při záručním plnění

Všichni zaměstnanci jsou a budou zavázáni povinností zachovávat důvěrnost a mlčenlivost, a to písemně.

Používaná IT infrastruktura bude poskytnuta v rámci cloudu (IaaS & PaaS) prostřednictvím Amazon Web Services (dále AWS). Kontrolu přístupu poskytne AWS provozovatel datového centra: Výpočetní střediska s nejvyšší bezpečností AWS používají kontrolní opatření odpovídají poslednímu stavu technických poznatků a několikastupňové kontrolní systémy. Výpočetní střediska jsou obsazena kvalifikovanými pracovníky v nepřetržitém provozu a přístup je přísně omezen na minimální práva a výlučně pro účely administrace systému.

Přístup k součástem hardwaru (clients) u TB Digital Services GmbH probíhá dle platných individualizovaných standardních opatření. Jedná se například o omezení přístupu osamocenými zařízeními (turnikety), kontrolními videosystémy, poplašným zařízením a/nebo ostrahou, elektronicky nebo mechanicky zabezpečenými dveřmi, budovou chráněnou proti vloupání, zdokumentovaným oprávněním k přístupu (návštěvy, externí pracovníci) nebo deklarovanými bezpečnostními úseky.

Kontroly přístupu zahrnují opatření týkající se zabezpečení zařízení, zabezpečení sítě a aplikací.

K zabezpečení zařízení ve vozidle jsou používána různá opatření: Mobilní koncová zařízení jsou pevně zabudována ve vozidle a jsou vybavena Secure Boot, tzn., že neexistuje možnost nahrávání a spouštění cizího operačního systému. Mobilní koncová zařízení komunikují s koncovým bodem kódovaně na základě individuálního certifikátu zařízení. Data jsou v rámci platformy RIO dále předávána kódovaná („Ubiquitous encryption“ nebo „encryption everywhere“). Koncová zařízení jsou pravidelně bezpečnostně aktualizována na nejnovější stav bezpečnosti (Patch-Management).

Jako opatření na zabezpečení sítě se rovněž používají různá standardní opatření: Jedná se o přiměřené (současnému stavu technických poznatků) odpovídající požadavky na hesla (délka hesla, komplexnost, doba platnosti apod.). Opakovaným chybným zadáváním identifikace uživatele / kombinace hesla povede k (dočasnému) zablokování údajů uživatele. Firemní síť je chráněna před nebezpečnými otevřenými sítěmi. Osvědčený je proces zajišťující pravidelné bezpečnostní aktualizace mobilních zařízení (OTA – proces). K odhalení nebo zabránění útokům na firemní síť (intranet) se používají vhodné technologie (např. Intrusion Detection Systeme). Pracovníci jsou pravidelně poučováni o rizicích a nebezpečích.

Jako opatření na zabezpečení aplikací se rovněž používají různá standardní opatření:

Příslušné aplikace jsou proti nežádoucímu přístupu chráněna přiměřenými mechanismy ověřování a autorizace. Jedná se o přiměřené (současnému stavu technických poznatků) odpovídající požadavky na hesla (délka hesla, komplexnost, doba platnosti apod.). Pro aplikace se zvláštní nutností ochrany jsou používány silné metody ověřování (např. token nebo PKI). Opakovaným chybným zadáváním identifikace uživatele / kombinace hesla povede k (dočasnému) zablokování údajů uživatele. Data používaní v příslušném procesu jsou na mobilně používaném zařízení k dispozici v kódované formě. Proběhlé přístupy a pokusy o přístup k aplikacím se protokolují. Vytvořené soubory s protokoly se po určitou vhodnou dobu (min. 90 dnů) archivují a (namátkově) kontrolují.

Uživatelská oprávnění (pro vstup a přístup) jsou zajištěna různými opatřeními, přičemž jsou zásadně přiřazena identifikovatelné osobě. Přidělování oprávnění je na odpovědnosti odpovědné osoby za platformu a pravidelně se kontroluje. Přidělování oprávnění ke vstupu probíhá dle určeného a zdokumentovaného postupu. Změny v přístupových oprávněních probíhají na principu čtyř očí a jsou zdokumentovány logfile v určité verzi.

Jako opatření na kontrolu přístupu nebo řízení se používají výlučně různá opatření: Přístupová práva se určují v rámci koncepce rolí a oprávnění a jsou zdokumentována a příslušným způsobem přiřazována určitým rolím dle požadavků úkolu. Zakládány jsou specifické role / oprávnění pro technické administrátory (kteří, pokud je to technicky možné, nemají žádný přístup k osobním datům). Zakládány jsou specifické role / oprávnění pro odbornou podporu (kteří nemají žádná technická administrátorská práva).

Definice rolí / oprávnění a přiřazení rolí / oprávnění probíhá, pokud je to technicky a organizačně možné, ne týmiž osobami a v kontrolně bezpečném (schvalovacím) procesu a je časově omezená. Přímé přístupy k databázi při uplatnění koncepce rolí / oprávnění jsou možné pouze autorizovanými administrátory databáze. Je upraveno používán soukromých datových nosičů, popř. je používání soukromých datových nosičů zakázáno. Jsou vydány závazné předpisy pro přístup k datům pro externí údržbu, dálkovou údržbu a činnosti. Probíhá likvidace/skartace dokumentů a datových nosičů (např. skartovačky, ochranné bedny) z hlediska ochrany osobních dat spolehlivou firmou.

Koncepce rolí a oprávnění se pravidelně upravuje dle měnící se struktury organizace práce (např. nové role) a přiřazené role / oprávnění se pravidelně kontrolují (např. nadřízenými) a přizpůsobují nebo odnímají. Probíhá pravidelná kontrola týkající se přidělených standardních profilů. Měnící se přístupy (zapisování, mazání) se protokolují a vytvořené soubory s protokoly se po určitou vhodnou dobu (min. 90 dnů) ukládají a (namátkově) kontrolují.

Jako obecná opatření pro zabezpečení předávání jsou používána různá standardní opatření:

Osoby pověřené předáváním dat jsou seznámeny předem s bezpečnostními opatřeními. Okruh příjemců je stanoven předem, aby byla možná odpovídající kontrola (autentizace). Celý proces předávání dat je určený a zdokumentován a provádění konkrétních předání dat se protokoluje a popřípadě zdokumentuje (např. potvrzení o přijetí, potvrzování). Osoby pověřené předáváním provedou nejprve kontrolu použitelnosti, úplnosti a správnosti.

Před prováděním konkrétního datového přenosu proběhne kontrola adresy příjemce (např. e-mailové adresy). Přenos dat po internetu probíhá kódovaně (např. kódováním souborů). Integrita předávaných dat, pokud je to technicky možné, je zajištěna použitím podpisů (digitální podpisy). Elektronické potvrzení přijetí se vhodnou formou archivuje. Nežádoucímu přenosu dat na internetu je zamezeno vhodnými technologiemi (např. Proxy, Firewall).

Dále se jako opatření pro oddělování používají následující standardní opatření:

Jsou k dispozici závazná pravidla týkající účelově vázaného zpracovávání pro dodržení nařízení o oddělování. Data získaná pro určité účely jsou ukládána zvlášť od dat získaných pro jiné účely. Používané IT systémy umožňují oddělené ukládání dat (schopností mandanta nebo koncepcí přístupu). Probíhá oddělování dat v systémech zkoušek a produktivity. U pseudonymizovaných dat jsou kódové můstky, které umožňují reidentifikaci, ukládány a archivovány odděleně. Při zpracovávání objednávky nebo přenosu funkce probíhá oddělení zpracovávání dat různých objednavatelů u dodavatele. Dostupné koncepce rolí a oprávnění umožňují svým řešením logické oddělení zpracovávaných dat.

4. Zajištění integrity při záručním plnění

Jako obecná opatření pro protokolování zadávání jsou používána různá standardní opatření:

Protokolují se změny přístupových práv a veškeré administrační činnosti. Zapisované přístupy (zadávání, změn, mazání) a změny v datových polích jsou protokolovány (např. obsah nově zadané nebo změněné sady dat). Probíhá protokolování informací (např. stahování) a protokolování přihlašování.

Používané podklady pro záznamy jsou dokumentovány pro dohledatelnost zadávání a archivovány. Protokolování probíhá s datem a časem, uživatelem, druhem aktivity, programem a pořadovým číslem sady dat. Nastavení protokolování se dokumentují.

Poskytuje se výlučně přístup k souborům protokolu pouze pro čtení. Okruh přístupových oprávnění k souborům protokolů je úzce omezen (např. na administrátora, osobu pověřenou ochranou dat, kontrolorem). Soubory protokolu se archivují pouze pro stanovenou dobu (např. 1 rok) a poté se dle práva na ochranu osobních dat mažou. Soubory protokolu se pravidelně automaticky vyhodnocují. Vyhodnocování souborů protokolů se pokud možno provádí v pseudonymizované formě.

5. Zajištění dostupnosti při záručním plnění

Architektura je zajištěna interními replikačními mechanismy v rámci platformy AWS proti ztrátě dat. Dále jsou používána následující opatření AWS pro zálohování objektů:

Jsou realizována protipožární opatření (např. protipožární dveře, detektory kouře, požární stěny, zákaz kouření). Výpočetní zařízení jsou chráněna proti záplavám (např. prostor výpočetního střediska je v 1. poschodí, hlásiče vody). Jsou prováděna opatření proti otřesům (např. prostor výpočetního střediska se nenachází v blízkosti dálnic, kolejí a strojoven). Výpočetní zařízení jsou zabezpečena proti elektromagnetickým polím (např. ocelovými deskami v obvodových stěnách). Jsou prováděna opatření proti vandalismu a krádežím (srov. kontrola přístupu). Výpočetní zařízení se nacházejí v klimatizovaných místnostech (teplota a vlhkost vzduchu jsou regulovány klimatizací). Výpočetní zařízení jsou chráněna přepěťovou ochranou proti přepěťovým špičkám. Jsou realizována opatření pro zabezpečení bezporuchového a nepřetržitého elektrického napájení (např. záložní zdroje UPS, nouzové agregáty).

Data jsou zálohována pravidelně formou záložních kopií v rámci AWS platformy. Koncepce zálohování je dokumentována a pravidelně kontrolována a aktualizována. Záložní média jsou chráněna před nepovoleným přístupem. Používané zálohovací programy odpovídají aktuálním standardům kvality a jsou pravidelně aktualizovány. Je zřízeno redundantní výpočetní středisko (vzdálené od místa zpracovávání) a v případě katastrofy je možné pokračovat se zpracováváním dat. Různá opatření pro kontrolu dostupnosti jsou zdokumentována v plánu krizového managementu AWS.

Pře vydáním příkazu ke zpracování dat je Dodavatel pečlivě zkontrolován dle určených kritérií (technická a organizační opatření). K tomu je především vyžadováno a kontrolováno doložení Dodavatelem prováděných technických / organizačních opatření na ochranu dat (zodpovězení katalogu otázek nebo koncepce ochrany dat). V závislosti na množství a citlivosti zpracovávaných dat probíhá toto ověřování případně i na místě u Dodavatele. Při výběru Dodavatelů jsou zohledňovány i vhodné certifikace (např. ISO 27001). Stanovení vhodnosti Dodavatele se zdokumentuje v přiměřené a dohledatelné formě.

Pro vznik obchodního vztahu se uzavře mezi objednatelem a dodavatelem smlouva o zpracovávání objednávek. Ta stanoví podrobně a písemně kompetence, odpovědnosti a také povinnosti obou stran. Pokud má pověřený poskytovatel služeb své sídlo mimo EU nebo Evropský hospodářský prostor, budou uplatněna standardní ustanovení EU. Je smluvně stanoveno, že zpracovávání dat Dodavatelem smí probíhat pouze v rámci pokynů ze strany Objednatele. Dodavatel je povinen Objednatele ihned upozornit na to, pokud by některým z jeho pokynů dle názoru Dodavatele porušil předpisy o ochraně dat. Pro dodržení práv dotčených osob se ve smlouvě o

zpracovávání dat objednávek dohodlo, že dodavatel objednateli poskytne přiměřenou součinnost, pokud to bude např. v případě poskytování informací dotčeným osobám nutné.

Při dalším průběhu zpracovávání objednávek objednatel zkontroluje výsledky práce dodavatele po formální a obsahové stránce. Dodržování technických a organizačních opatření se pravidelně kontroluje. K tomu se použije především předložení aktuálních osvědčení nebo vhodných certifikací, popř. se prokážou provedené kontroly bezpečnosti IT a ochrany dat. Pokud bude využit subdodavatel, je smluvně dohodnuto, že bude příslušným způsobem kontrolován.

6. Zajištění zatížitelnosti systému při záručním plnění

Cloudová infrastruktura AWS byla vytvořena jako jedna z nejflexibilnějších a nejbezpečnějších cloudových počítačových prostředí. Byla koncipována jako optimum pro dostupnost a kompletní oddělení zákazníků. Poskytuje extrémně širokou, vysoce provozně bezpečnou platformu, umožňující zákazníkům používání aplikaci a obsahů v případě potřeby rychle a bezpečně po celém světě. AWS-Services jsou maximálně nezávislé na obsahu, aby všem zákazníkům mohly nabídnout vysokou úroveň bezpečnosti, bez ohledu na druh obsahu nebo geografický region, v němž je obsah ukládán.

Výpočetní střediska s nejvyšší bezpečností AWS světové úrovně, používají kontrolní opatření odpovídají poslednímu stavu technických poznatků a několikastupňové kontrolní systémy. Výpočetní střediska jsou obsazena kvalifikovanými pracovníky v nepřetržitém provozu a přístup je přísně omezen na minimální práva a výlučně pro účely administrace systému.

7. Postupy pro obnovení dostupnosti osobních dat dle fyzických nebo technických podmínek

Výpočetní střediska AWS jsou zřizována v clustrech v různých oblastech světa. Všechna výpočetní střediska jsou online a poskytují služby zákazníkům; žádné výpočetní středisko není odpojené. Při výpadku přesunou automatické procesy zpracovávání dat zákazníků mimo zasaženou oblast. Klíčové aplikace jsou k dispozici v konfiguraci N+1, aby v případě výpadku výpočetního střediska byla k dispozici dostatečná kapacita pro přesunutí datového provozu na ostatní místa.

AWS nabízí flexibilitu, umisťování instancí a dat v rámci několika geografických regionů a ukládání prostřednictvím několika Availability Zones v rámci jednotlivých regionů. Každá Availability Zone byla vyvinuta jako nezávislá výpadková zóna. To znamená, že Availability Zones jsou v rámci typického městského regionu fyzicky rozdělené a nacházejí se např. v oblastech s nižším rizikem záplav (dle regionu se liší kategorizace záplavových oblastí). Dále se k vlastním nepřerušovaným zdrojům elektrického napájení a generátorům nouzového proudu na místě připojují všechny Availability Zones přes různé napájecí sítě nezávislých zdrojů elektrického napájení, aby se minimalizovala individuální chybová místa. Všechny Availability Zones jsou redundantní s několika poskytovateli Tier-1-Transit providery.

Tým Amazon využívá ke správě případů běžné diagnostické postupy na odstranění kritických jevů. Provozní personál nabízí nepřetržitou službu, dvacet čtyři hodin denně, sedm dnů v týdnu a 365 dnů v roce pro detekci poruch a odstranění jejich příčin a následků.

8. Postupy pravidelné kontroly, hodnocení a evaluace účinnosti technických a organizačních opatření

Směrnice ve firmě a pokyny, popř. implementované standardy týkající se bezpečnosti informací, se uplatňují i s ohledem na zavádění a provoz platformy RIO. Provozní funkce na ochranu dat a bezpečnost informaci jsou k dispozici (osoba pověřená ochranou dat a Information Security Officer). Zaměstnanci jsou vázání mlčenlivostí týkající se dat a jsou informováni o opatřeních z hlediska bezpečnosti dat a IT bezpečnosti formou brožur, letáků, interních pokynů apod.

Interní procesy se kontrolují z hlediska dodržování technických a organizačních opatření pro bezpečnost dat revizemi, zabezpečení informací a ochrana dat.

Zpracovávání a opatření z hlediska bezpečnosti dat jsou zdokumentována v soupisu činností pro zpracovávání. Pravidelně probíhá kontrola účinnosti opatření (interní a externí).