Feldolgozási megbízási szerződés
(a DS-GVO 28. cikke alapján)

amely létrejött:

a **Felhasználó** (a főszerződésben meghatározottak szerint)

(továbbiakban: „**Megbízó**“)

és

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

(továbbiakban: „**Megbízott**“)
között (a Megbízó és a Megbízott megnevezése a továbbiakban külön „**Fél**“ és együttesen „**Felek**“).

Preambulum

(A) Jelen feldolgozási megbízási szerződés (továbbiakban: „**szerződés**“) minden olyan tevékenységre vonatkozik, melyek során a Megbízott a Megbízó, harmadik fél vagy egyéb érintett személyre vonatkozó adataival (mint az 1.5 pontban lent meghatározottak szerint) a 2 pontban leírt tevékenységgel összefüggésben az platformhasználat és adott esetben az ezalatt a további szolgáltatásokra vonatkozó megkötött egyéni szerződések Általános Keretfeltételeiből (továbbiakban: „**főszerződés**“) érintkezik.

(B) Jelen szerződésben a Megbízó felelősként és a Megbízott feldolgozási megbízottként egy feldolgozási megbízási szerződés keretében a német Adatvédelmi törvény Általános adatvédelmi rendelet 28. cikkely szerint (a lenti meghatározásnak megfelelően) tevékenykednek.

A Felek ezért a következőkben állapodnak meg:

1 Meghatározások és értelmezések

1.1 „**Európai jog**“ az Európai Unió alkalmazható joga, az Európai Unió jelenlegi tagállamainak alkalmazható törvényei, valamint minden egyes olyan állam alkalmazható törvényei, amely utólag válik az Európai Unió tagállamává.

1.2 „**Európai adatvédelmi jog**“ az Európai Unió alkalmazható joga személyi adatok feldolgozására (különösen az Általános adatvédelmi rendelet), az Európai Unió jelenlegi tagállamainak alkalmazható törvényei a személyi adatok feldolgozására vonatkozóan (különösen a német Adatvédelmi törvény mindenkor érvényes változata), valamint minden egyes olyan állam alkalmazható törvényei a személyi adatok feldolgozására vonatkozóan, amely utólag válik az Európai Unió tagállamává.

1.3 „**DS-GVO**“ az EURÓPAI PARLAMENT ÉS TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok feldolgozása tekintetében történő védelméről és az ilyen

adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (Általános adatvédelmi rendelet)“.

1.4 „**BDSG**“ a német Adatvédelmi törvény.

1.5 „**Személyre vonatkozó adatok**“ jelentése a német adatvédelmi törvény/ az Általános adatvédelmi rendelet meghatározása szerint.

2 Az adatfeldolgozás tárgya / A megbízó kötelezettségei

2.1 Jelen szerződés szabályozza a Felek kötelezettségeit a Megbízó személyre vonatkozó adatainak Megbízott általi feldolgozásával összefüggésben az 1. számú mellékletben megnevezett főszerződés keretében.

2.2 A feldolgozás tárgya és időtartama, a feldolgozás módja és célja, a személyre vonatkozó adatok fajtája, az érintett személyek kategóriái és a felelős kötelezettségei és jogai jelen szerződés 1. számú mellékletéből és a főszerződés szolgáltatásának leírásából következnek.

2.3 A megbízó az Általános adatvédelmi rendelet szempontjából felelős marad az adatfeldolgozásért, és biztosítja, hogy megengedhető legyen az érintett személyek (sofőrök és adott esetben további személyek) személyre vonatkozó adatainak feldolgozása. A megbízó különösen megfelel az információszolgáltatásra vonatkozó széles körű kötelezettségeinek, és biztosítja, hogy a személyre vonatkozó adatok feldolgozása adatvédelmi jogon alapuljon (például egy vállalati megállapodás megkötése, a feldolgozás korlátozása foglalkoztatás céljából).

3 A Megbízott kötelezettségei

3.1 A Megbízott a Megbízó személyre vonatkozó adatait kizárólag az 1. számú mellékletben megnevezett célokra és a főszerződés keretében, valamint a Megbízó megbízásából és az 1. számú mellékletben dokumentált utasításai szerint dolgozza fel; a Megbízott a személyre vonatkozó adatokat jelen szerződés érvényességi ideje alatt más célokra nem dolgozza fel. Ez az adatfeldolgozást a jelen szerződésen kívül a főszerződés 8.3.4 pontja szerint saját célokra nem érinti. A személyre vonatkozó adatokról másolatok vagy másodlatok a Megbízó tudta nélkül nem készülnek. Ez alól kivételt képeznek a biztonsági másolatok, amennyire azok a szabályos adatfeldolgozás biztosításához szükségesek, valamint olyan adatok, melyek a törvényi tárolási kötelezettségek betartása miatt szükségesek.

3.2 Az adatfeldolgozási szolgáltatások teljesítésének befejeztével a Megbízottnak a Megbízó valamennyi személyre vonatkozó adatát választása szerint vagy át kell adnia és/vagy magánál az adatvédelmi törvénynek megfelelően törölnie kell, amennyiben ezzel a törvényi megőrzési időszakok nem állnak szemben és amennyiben a Megbízott azokat jelen szerződésen kívül a főszerződés 8.3.4 pontja szerint

saját célra nem dolgozza fel. Ugyanez vonatkozik a tesztelés és a selejtezés anyagára is. Az adatok teljes törlését, ill. a Megbízónak való kiadását a dátum feltüntetésével írásban igazolni kell.

3.3 Ami a szolgáltatások körét illeti, a Megbízott a Megbízó utasításainak megfelelően támogatja a Megbízót az adatalanyok jogainak teljesítésében (tájékoztatás, javítás, elutasítás, törlés).

3.4 A Megbízott igazolja azt, hogy ő - amennyiben a törvényi szabályozás szerint szükséges - üzemi adatvédelmi megbízottat nevezett ki (vesd össze a német Adatvédelmi törvény 38. §-val és az Általános adatvédelmi rendelet 37. cikkelyével).

3.5 A Megbízott kötelezi magát arra, hogy a Megbízóval az adatvédelmi hatóságok ellenőrzéseinek eredményét haladéktalanul megismerteti, amennyiben azok a Megbízó adatainak feldolgozásával összefüggenek. Az esetlegesen megállapított kifogásokat a Megbízottnak méltányos határidőn belül javítania kell és ezt a Megbízóval közölnie kell.

3.6 A Megbízott általi és a Megbízó által engedélyezett alvállalkozók általi adatfeldolgozás kizárólag a Német Köztársaság területén, az Európai Unió egy tagállamában vagy az Európai Gazdasági Közösségről szóló egyezmény másik szerződött államában történik. Bármely más országban való áthelyezéshez (továbbiakban: „**harmadik ország**“) a Megbízó előzetes kifejezett hozzájárulása szükséges és ezen kívül csak akkor történhet meg, ha teljesítik a harmadik országokba irányuló adatexportálás különös előfeltételeit (vesd össze az Általános adatvédelmi rendelet 40. cikkelyével). Ehhez az 1. számú mellékletben lévő adatok szükségesek és adott esetben mellékelni kell a kiegészítő szerződéses dokumentumokat.

3.7 A Megbízottnak a munkák elvégzésénél foglalkoztatott munkatársaival meg kell ismertetnie az irányadó adatvédelmi rendelkezéseket és köteleznie kell őket az adattitokra (vesd össze az Általános adatvédelmi rendelet 28. cikkely 3b) bekezdésével), valamint arra alkalmas lépésekkel biztosítani kell azt, hogy azok a munkatársak személyre vonatkozó adatokat csak a Megbízó utasítására dolgozhassanak fel.

3.8 A Megbízott a szerződés teljes futamideje alatt rendszeresen felügyeli jelen szerződés adatvédelmi előírásainak és a Megbízó dokumentált utasításainak betartását. Az ellenőrzések eredményét a Megbízónak kérésre be kell mutatni, amennyiben azok a Megbízó adatainak feldolgozásánál lényegesek. A felügyeleti intézkedéseket egy adatvédelmi koncepcióban írták le, melyet a Megbízónak kérésre be kell mutatni.

3.9 A Megbízottnak a Megbízót tekintettel a feldolgozás módjára és lehetőség szerint arra alkalmas technikai és szervezési intézkedésekkel támogatnia kell abban, hogy teljesítse az érintett személyeknek az Általános adatvédelmi rendelet III. fejezetében megnevezett jogai gyakorlására vonatkozó kérelmek megválaszolási kötelezettségét. A Megbízónak kell a Megbízottnál keletkezett költségeket viselnie.

3.10 A Megbízottnak a Megbízót tekintettel a feldolgozás módjára és a részére rendelkezésre álló információkra az Általános adatvédelmi rendelet 32-36 cikkelyeiben megnevezett kötelezettségek betartásánál.

4 Adatbiztonsági technikai és szervezési intézkedések

4.1 A Megbízottnak méltányos adatvédelmi technikai és szervezési intézkedéseket kell végrehajtania (vesd össze az Általános adatvédelmi rendelet 32. cikkelyével). A Megbízott különösen köteles jelen szerződés 2. számú mellékletében a szerződés szerint egyeztetett technikai és szervezési intézkedéseket megvalósítani. Ezeket az intézkedéseket a Megbízottnak a megbízási jogviszony folyamán a technikai és szervezési továbbfejlesztéshez kell igazítania, anélkül hogy ennek során a védelmi szintet csökkentené. A lényeges változásokról írásban kell megállapodni.

4.2 A Megbízott a Megbízónak kérésre a technikai és szervezési intézkedések tényleges betartását igazolja.

4.3 A Megbízott köteles az adatfeldolgozásról megfelelő dokumentációt vezetni, amely alapján a Megbízó a szabályos adatfeldolgozási igazolást kiadhatja. Az igazolás történhet engedélyezett tanúsítási eljárással is az Általános adatvédelmi rendelet 42. cikkelye szerint is.

5 Alvállalkozók

5.1 A Megbízottnak ezúton engedélyezték az 1. számú mellékletben megnevezett alvállalkozók bevonását.

5.2 További alvállalkozók bevonását ezúton általánosan engedélyezik. A Megbízott a Megbízót azonban tájékoztatni fogja az alvállalkozók bevonására vagy pótlására vonatkozó minden tervezett változtatásról; a Megbízó a tervezett változtatások ellen ellenvetést nyújthat be. Nem számítanak alvállalkozói jogviszonynak jelen szabályozás szerint azok a szolgáltatások, melyeket a Megbízott harmadik félnél mellékszolgáltatásként támogatásként a megbízás végrehajtásánál igénybe vesz. Ide tartoznak például a telekommunikációs szolgáltatások, takarító munkatársak, adathordozók ellenőrei vagy az adathordozók ártalmatlanítása. A Megbízott azonban köteles a Megbízó adatai védelmének és biztonságának biztosítására kiadott mellékszolgáltatásoknál is méltányos és törvényeknek megfelelő szerződéses megállapodásokat kötni, valamint ellenőrzési intézkedéseket végrehajtani.

5.3 Ha a Megbízott alvállalkozót vesz igénybe, akkor a Megbízottnak biztosítania kell azt, hogy az alvállalkozóra (i) egy az alvállalkozó és a Megbízott között megkötendő szerződésben vagy (ii) az európai adatvédelmi jog szerinti egyéb jogi eszközzel ugyanazokat az adatvédelmi kötelezettségeket terheljék, melyek a Megbízottat jelen szerződés szerint terhelik. Ennek során különösen azt kell biztosítani, hogy az alvállalkozó elegendő garanciákat kínáljon ahhoz, hogy az alkalmas technikai és szervezési intézkedéseket úgy végezzék el, hogy a személyre vonatkozó adatok feldolgozása az Általános adatvédelmi rendelet követelményeinek megfelelően történjen. A Megbízó írásbeli kérésére a Megbízott

a Megbízónak tájékoztatást ad a szerződés lényeges tartalmáról és az adatvédelmi szempontból lényeges kötelezettségek végrehajtásáról alvállalkozói jogviszonyban, szükség esetén a vonatkozó szerződési dokumentumokba való betekintéssel. A kereskedelmi feltételeket a Megbízott kitakarhatja. A Megbízó köteles a megkapott információkat titokban tartani.

6 Ellenőrzési jogok

6.1 A Megbízónak joga van, a jelen szerződésből eredő kötelezettségek betartását (ideértve a kiadott utasításokat) saját maga vagy a Megbízó által megnevezett harmadik személy által ellenőrizni, ill. ellenőriztetni.

6.2 A Megbízott biztosítja a Megbízónak a megfelelő támogatást az ellenőrzéseknél. A Megbízott különösen az adatfeldolgozási mellékletekhez biztosítja a hozzáférést és megadja a szükséges tájékoztatást.

6.3 Arra az esetre, ha az ellenőrzés arra az eredményre vezet, hogy a Megbízott és/vagy az adatfeldolgozás nem tartja be jelen szerződés és/vagy az európai adatvédelmi jog előírásait, akkor a Megbízott valamennyi olyan javítási intézkedéseket fog végrehajtani, melyek ahhoz szükségesek, hogy biztosítsák jelen szerződés és/vagy az európai adatvédelmi jog előírásait.

6.4 Azokat a költségeket, melyek a Megbízónál az ellenőrzés végrehajtásánál keletkeznek, magának kell viselnie. Azokat a költségeket, melyek a Megbízottnál a Megbízó általi ellenőrzés végrehajtásánál keletkeznek, követelheti a Megbízótól, amennyiben a Megbízó egy naptári évben egynél többször végzi, ill. végezteti el az ellenőrzést.

6.5 A Megbízottnál végzendő ellenőrzéseket időben be kell jelenteni és azok aránytalanul nem akadályozhatják a Megbízott üzletmenetét.

7 Figyelemfelhívási kötelezettségek

A Megbízott haladéktalanul tájékoztatja a Megbízót arról, ha egy a Megbízó által kiadott utasítás a Megbízott véleménye szerint megsérti az európai adatvédelmi jogot. A jogosan kifogásolt utasítást nem kell követni, amíg azt a Megbízó nem változtatja meg vagy kifejezetten nem igazolja. A Megbízott nem köteles az utasítások anyagi-jogi ellenőrzésére.

A Megbízott a hibák megállapítása vagy az adatfeldolgozás szabálytalanságai vagy adatvédelem megszegésének gyanúja esetén (együttesen továbbiakban: egy „**esemény**“) a Megbízót haladéktalanul megfelelően tájékoztatni kell. A Megbízónak az eseményt minden tényállási körülménnyel, hatásaival és valamennyi elhárítási intézkedéssel dokumentálnia kell és a Megbízó kérésére ezeket a dokumentált információkat írásban vagy elektronikusan a Megbízónak haladéktalanul továbbítani kell.

8 Felelősség és felmentés

8.1 A Megbízott felel azokért a károkért, melyeket a Megbízott vagy teljesítési segédei szándékosan és/vagy durva gondatlansággal okoztak. Azokért a károkért, melyek a Megbízott vagy teljesítési segédei egyszerű gondatlanságán alapulnak, a Megbízó csak akkor felel, amennyiben azzal egy lényeges kötelezettséget szeg meg. A lényeges kötelezettségek olyan szerződési kötelezettségek, amelyek a szerződés szabályos végrehajtását lehetővé teszik és azok teljesítésére a Megbízott hagyatkozott és hagyatkozhatott. Egyszerű gondatlanság esetén az ilyen lényeges kötelezettségek megszegésénél a Megbízott felelőssége a jellemzően előre látható károkra korlátozódik.

8.2 A Megbízó a Megbízottat felmenti harmadik fél valamennyi igénye, kára vagy kiadásai alól (ideértve az érintett személyeket és/vagy az adatvédelmi hatóságokat), melyek a Megbízó jelen szerződés és/vagy az európai adatvédelmi jog rendelkezéseinek megszegésén alapulnak; ez nem érvényes akkor, amennyiben a Megbízó nem hibás a szabályszegésben vagy a Megbízott a szabályszegéshez hozzájárult.

9 Futamidő

Jelen szerződés futamideje megfelel a fő szerződés futamidejének. A fő szerződés bármilyen okból való megszűnésével jelen szerződés is automatikusan megszűnik. A fontos okból való felmondást ez nem érinti.

10 Egyéb

10.1 A megbízott jelen szerződés szerinti szolgáltatásait a fő szerződésben meghatározott díjazási szabályozás fedezi.

10.2 Ha a Megbízó személyre vonatkozó adatait a Megbízottnál harmadik fél intézkedései (zálogba vétel vagy lefoglalás), csőd vagy egyezségi eljárás vagy egyéb ehhez hasonló esemény veszélyezteti, arról a Megbízottnak a Megbízót haladéktalanul tájékoztatnia kell.

10.3 Ha jelen szerződés egyes rendelkezései érvénytelenek lennének vagy azzá válnának, az a többi rendelkezés érvényességét nem érinti. A Felek egy záradék érvénytelensége esetén megállapodnak egy tárgyi és gazdasági szempontból a szerződés célja szerint kialakított pótszabályozásban.

10.4 Arra az esetre, ha Nagy-Britannia kiválik az Európai Unióból, a Megbízott kötelezi magát arra, hogy már most megköt minden olyan megállapodást és megtesz minden olyan intézkedést, melyek ahhoz szükségesek, hogy a szerződés tárgyát képező adatfeldolgozást Nagy-Britanniában a kiválás időpontjából kezdődően adatvédelmi jogi szempontból engedéllyel végezzék. Amennyiben a kiválás időpontjában nem rendelkeznek az Európai Bizottság pozitív megfelelőségi döntésével, ezek mai szempontból különösen a standard adatvédelmi záradékok a 46. cikkely 2c) bekezdése szerint a

személyre vonatkozó adatok olyan megbízott adatfeldolgozóknak való továbbítására vonatkozóan, akik harmadik országokban rendelkeznek székhellyel, melyekben nincs biztosítva a megfelelő védelmi szint.

Ha a Megbízott jelen kötelezettségeit nem teljesíti, akkor a Megbízónak joga van, a Megbízottól Nagy-Britannia Európai Unióból való kiválásától kezdődő hatállyal megkövetelni azt, hogy az érintett szolgáltatásokat az Európai Unió területén lévő állandó székhellyel rendelkező kapcsolt vállalkozás, ill. részvállalkozás végezze el, anélkül hogy a Megbízónak többletráfordítása vagy kiegészítő költségei keletkeznek.

10.5 Jelen feldolgozási megbízási szerződés 18 nyelvi változatban áll rendelkezésre, eltérések esetén a német eredeti változat élvez elsőbbséget.

10.6 Jelen szerződésre a Német Szövetségi Köztársaság joga vonatkozik az ENSZ vételi jog kizárásával. A kizárólagos bírói illetékesség helye München.

10.7 A következő mellékletek a szerződés részét képezik:

1. számú melléklet – a feldolgozási megbízás leírása
2. számú melléklet – Technikai és szervezési intézkedések

1. SZÁMÚ MELLÉKLET – A feldolgozási megbízás leírása

1 Főszerződés

Főszerződés a szerződés fő részének 2.1 pontja 2.1 értelmében a „Platformhasználat általános keretfeltételei“.

Címek/ Felek: a **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 München / **Felhasználó**

2 A megbízás tárgya és időtartama

A megbízás tárgya a főszerződés 1. pontjából (*Tárgy*) és 8. pontjából (*A felhasználó adatai és az adatvédelem*) adódik; a megbízás időtartama a főszerződés 7. pontjából (*Szerződés megkötése, szerződés időtartama és felmondási jogok*) adódik.

3 Az adatfeldolgozás/ az adatfeldolgozási intézkedések terjedelme, módja és célja

A személyre vonatkozó adatok feldolgozásának terjedelme, módja és célja a főszerződés 8. pontjából adódik.

A szerződés tárgyának részletesebb leírása a terjedelemre, módra és célra való tekintettel

Annak érdekében, hogy a Megbízott által kínált szolgáltatásokat (a főszerződésben meghatározottak szerint) elvégezhessék, a Megbízottnak a Megbízó összekapcsolt járművekről és a mobil eszközökről szóló személyre vonatkozó adatait (adott esetben harmadik szolgáltató által, amellyel a felhasználó harmadik fél általi szolgáltatásban egyezett meg, továbbított személyre vonatkozó adatok) a szolgáltatások teljesítéséhez elfogadható mértékben összegyűjti és a Megbízott platformjára továbbítja és ott tárolja. A Megbízott a platformon tárolt adatokat a szolgáltatás elvégzéséhez szükséges mértékben dolgozza fel (például azért hogy a személyre vonatkozó adatok alapján a sofőrök vezetési viselkedése, valamint az összekapcsolt járművek, valamint a mobil eszközök használatát elemezze és kiértékelje és a Megbízónak erre alapozva olyan speciálisan rá szabott ajánlatokat, mint a sofőrök oktatása, felszerelési részletek, valamint a hatékonyságnövelési javaslatok készítsen). A pontos terjedelem, mód vagy cél különösen a kiegészítésképpen megkötendő egyedi szerződésekből adódnak.

4 Az érintettek köre (érintett személyek kategóriái)

A feldolgozási megbízási szerződés a következő személyi köröket érinti:

- **Sofőrök és a többi munkatárs** (a Megbízó saját társaságának munkatársai), pl.: munkavállalók, tanulók, pályázók, egykori foglalkoztatottak
- **olyan sofőrök**, akik nem munkatársak;
- **kapcsolattartó személyek** a berakodóknál/ kirakodóknál vagy a Megbízó egyéb üzletfeleinél; és
- **konszern-munkatársaknál** (a Megbízó csoportja másik társaságának munkatársai).

5 A személyre vonatkozó adatok fajtája

A feldolgozási megbízás a személyre vonatkozó adatok következő fajtáit foglalja magába:

- A sofőr neve és vezetői azonosítószáma;
- A jármű azonosítószáma;
- Telephelyadatok;
- A vezetési időre és a pihenőidőre vonatkozó adatok;
- A vezetési viselkedés adatai;
- Az összekapcsolt járművek állapotára vonatkozó adatok;
- Pótkocsi állapotára vonatkozó adatok;
- Felépítmények, ill. hozzáépítések, aggregátok és további járműrészek állapotára vonatkozó adatok;
- Az adott esetben a kapcsolt, a tárgyak internetével kapcsolatos eszközök állapotának adatai
- A mobileszközök állapotának adatai;
- Rakodási adatok;
- Megbízási adatok és
- A berakodók/ kirakodók vagy a Megbízó egyéb üzletfelei kapcsolattartó személyeinek kapcsolattartási adatai.

6 Dokumentált utasítások

A Megbízó a Megbízott ezúton arra utasítja, hogy a személyre vonatkozó adatokat a főszerződés 8. pontjának megfelelően dolgozza fel. Ez különösen a következő adatfeldolgozást foglalja magába:

- A személyre vonatkozó adatokat az összekapcsolt járműveken vagy a mobileszközökön keresztül a Megbízó felhő-alapú platformján keresztül továbbítják és ott tárolják.
- A személyre vonatkozó adatokat jelen szerződésben csak feldolgozzák, amennyiben az a főszerződés teljesítéséhez szükséges; ez a főszerződés 8.3.4 pontját nem érinti.
- A Megbízott a személyre vonatkozó adatokat harmadik félnek továbbítja (a főszerződésben meghatározottak szerint), amennyiben harmadik szolgáltatónak való ilyen továbbítás szükséges, azért hogy a harmadik fél szolgáltatásait (a főszerződésben meghatározottak szerint) a Megbízónál elvégezhesse.
- A Megbízott a személyre vonatkozó adatok alapján a sofőrök vezetési viselkedése, valamint az összekapcsolt járművek, valamint a mobil eszközök használatát elemezi és kiértékeli és a Megbízónak erre alapozva olyan speciálisan rá szabott ajánlatokat, mint a sofőrök oktatása, felszerelési részletek, valamint a hatékonyságnövelési javaslatok készít.

7 A feldolgozás helye

- Németország.
- Egyesült Királyság; amennyiben az informatikai rendszerek erőforrásainak szolgáltatási és/ vagy informatikai rendszerek támogatási céljaira az Európai Unión belül adatokat dolgoz fel, a megfelelő feldolgozási megbízási szerződéseket kötötték meg.
- Amennyiben a Megbízott az informatikai rendszerek erőforrásainak szolgáltatási és/ vagy informatikai rendszerek támogatási céljaira az Európai Unión kívül (ehhez vesd össze az 1. számú melléklet8. pontját) alvállalkozókat alkalmaz, akkor a személyre vonatkozó adatok továbbítása a Megbízott és az alvállalkozó között megkötött, az Általános adatvédelmi rendelet 46. cikke (2) bekezdésének c) pontjával összhangban a személyes adatok harmadik fél általi feldolgozására vonatkozó szabványos szerződéses kikötések/szabványos adatvédelmi záradékok szerint történik.

8 Alvállalkozók

A Megbízott a következő alvállalkozókat (akik adott esetben további alvállalkozókat alkalmazhatnak) alkalmazza:

Sz.	Alvállalkozó (cégnév, cím, kapcsolattartó személy)	Feldolgozott adatkategóriák	Adatfeldolgozási lépések/ az alvállalkozói feldolgozás célja
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	A platform valamennyi személyre vonatkozó adata, amely az értékesítési résszel foglalkozik (vagyis ahol az ügyfél a platformon regisztrálhat és rendelhet).	Platform-szolgáltatás
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	A platform valamennyi személyre vonatkozó adata, amely az értékesítési résszel foglalkozik (vagyis ahol az ügyfél a platformon regisztrálhat és rendelhet).	Informatikai rendszerek támogatása a platformra vonatkozóan
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 USA https://aws.amazon.com/de/compliance/contact/	Valamennyi egyéb személyre vonatkozó felhasználói adat, melyet a járműről a Megbízottnak továbbítanak.	Platform-szolgáltatás / informatikai rendszerek támogatása a platformra vonatkozóan
4	Adott esetben a jövőben a 3. számú helyett: Amazon Webservices (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 USA https://aws.amazon.com/de/compliance/contact/	Valamennyi egyéb személyre vonatkozó felhasználói adat, melyet a járműről a Megbízottnak továbbítanak.	Platform-szolgáltatás
5	MAN Service und Support GmbH Dachauer Straße 667 80995 München	Valamennyi személyre vonatkozó adat, melyek az ügyfelek ajánlatkéréseinek feldolgozásához az 1. szintű és a 2. szintű támogatás	1. szintű támogatás

	Németország	keretében szükséges.	
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 USA	Valamennyi személyre vonatkozó adat, melyek az a számlakiállítás/ megbízás lebonyolításának feldolgozásához szükséges.	Platform-szolgáltatás (EU Tenant – Tárolja az Amazon Web Services (EU) – lásd a 4. pontot
7	MAN Truck & Bus AG Dachauer Str. 667 80995 München Németország	Valamennyi egyéb személyre vonatkozó felhasználói adat, melyeket az összekapcsolt járművekről és/ vagy a mobileszközökről továbbítanak a Megbízottnak.	Platform-szolgáltatás
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Németország	Valamennyi egyéb személyre vonatkozó felhasználói adat, melyet a TBM1/2 járművekről a Megbízottnak továbbítanak.	Platform-szolgáltatás
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Svédország	Valamennyi egyéb személyre vonatkozó felhasználói adat, melyet a járműről a Megbízottnak továbbítanak.	Platform-szolgáltatás
10	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hannover Németország	Valamennyi egyéb személyre vonatkozó felhasználói adat, melyet a járműről a Megbízottnak továbbítanak.	Platform-szolgáltatás

2. számú MELLÉKLET – Technikai és szervezési intézkedések
A Megbízott által végrehajtandó technikai és szervezési intézkedéseket - a kockázatnak megfelelő védelmi szint biztosítása érdekében - a RIO platformra vonatkozó adatvédelmi koncepcióban került leírásra és különösen a következőket tartalmazza:

1. Álnévhasználat

Amennyiben a személyre vonatkozó adatokat olyan kiértékelési célokra használják, melyek az álnevesített adatokkal és végrehajthatók, ott álnevesítési technikákat alkalmaznak. Ennek során először minden adatmezőt előre meghatároznak, hogy kell-e álnevesíteni, mert ez lehetővé tenné a személy kikövetkeztethetőségét. Az álnevesítési kulcsot egy „adatszéfben" helyezik el, amihez a lehetséges maximális hozzáférési korlátozást állítják be.

2. Titkosítás

A mobil végkészülékek titkosítva kommunikálnak a végponttal a készülékre egyénileg jellemző készüléktanúsítvány alapján. Az adatokat a RIO platformon belül titkosítva továbbküldik („Ubiquitous encryption" oder „encryption everywhere").

3. A megbízhatóság biztosítása

Minden munkatársnak felhívták a figyelmét titoktartási kötelezettségére és írásban kötelezték az adattitok megtartására.

A felhasznált informatikai rendszer infrastruktúrát az Amazon Web Services-en (a továbbiakban AWS) keresztül felhő formájában bocsátják rendelkezésre. A belépési ellenőrzést az AWS adatközpont-üzemeltető bocsátja rendelkezésre: a magas biztonsági szintű AWS számítógépközpontok aktuális műszaki szintű elektronikus felügyeleti intézkedéseket és több fokozatú hozzáférési ellenőrzési rendszereket alkalmaznak. A számítógépközpontokat a teljes időszakra képzett biztonsági személyzettel látják el és a hozzáférést szigorúan a legkisebb jogok elve alapján és kizárólag rendszeradminisztrációs célokra biztosítják.

A hardverelemekhez (kliensek) való hozzáférés a TB Digital Services GmbH cégnél az érvényes, az egyes esetben alkalmas standard intézkedések szerint történik. Ezek például a két személy egyidejű áthaladását megakadályozó berendezéseken (forgóvillák) keresztüli belépési korlátozások, videómegfigyelő berendezések, riasztóberendezések és/vagy őrszolgálat, elektronikusan vagy mechanikusan biztosított ajtók, betörés ellen biztosított épületek, dokumentált belépési jogosultságok (látogatók, idegen munkaerők) vagy deklarált biztonsági területek.

A beléptetési ellenőrzések magukba foglalják a készülékbiztosítási, a hálózatbiztosítási és az alkalmazásbiztosítási intézkedéseket.

A készülékbiztosítás intézkedéseként a járműben a következő intézkedéseket alkalmazzák: A mobil végkészülékeket a járművekbe beépítették és biztonsági boottal rendelkeznek, vagy nincs lehetőség arra, hogy idegen operációs rendszer töltődjön be és induljon el. A mobil végkészülékek titkosítva kommunikálnak a végponttal a készülékre egyénileg jellemző készüléktanúsítvány alapján. Az adatokat a RIO platformon belül titkosítva továbbküldik („Ubiquitous encryption" vagy „encryption everywhere"). A végkészülékek a biztonsági frissítések rendszeres importálásával az aktuális biztonsági szinten vannak (patch-menedzsment).

Hálózatbiztosítási intézkedésként éppúgy különböző standard intézkedéseket alkalmaznak: Megfelelő (a technika állásának megfelelő) jelszóelőírásokat implementálnak (jelszó hossza, komplexitása, érvényességi ideje, stb.). A felhasználó-azonosítás/ jelszókombináció ismételt hibás beírása a felhasználó-azonosítás (átmeneti) zárolásához vezet. A vállalati hálózatot egy tűzfal védi a nem biztonságos nyílt hálózatokkal szemben. Egy folyamat működik, amely a mobil készülékek biztonsági frissítéssel való rendszeres ellátását (OTA-folyamat) biztosítja. A vállalati hálózatra irányuló támadások felderítéséhez, ill. elkerüléséhez (Intranet) arra alkalmas technológiákat (pl.: Intrusion Detection rendszerek). A munkatársakat rendszeresen érzékenyítik a veszélyekre és kockázatokra vonatkozóan.

Alkalmazásbiztonsági intézkedésekként néhány standard intézkedést alkalmaznak:

A lényeges alkalmazásokat megfelelő hitelesítési és jogosultság-megállapítási mechanizmusok az illetéktelen hozzáférés ellen biztosították. Megfelelő (a technika állásának megfelelő) jelszóelőírásokat implementálnak (jelszó hossza, komplexitása, érvényességi ideje, stb.). A különös védelmi igényű alkalmazásokhoz erős hitelesítési mechanizmusokat használnak (pl.: token, PKI). A felhasználó-azonosítás/ jelszókombináció ismételt hibás beírása a felhasználó-azonosítás (átmeneti) zárolásához vezet. A lényeges eljárásban felhasznált adatok titkosított formában egy mobil adathordozón vannak. Az alkalmazásokba történt belépéseket és belépési kísérleteket jegyzőkönyvezik. Az elkészült jegyzőkönyvfájlokat alkalmas időszakra (legalább 90 nap) tárolják és (szúrópróbaszerűen) ellenőrzik.

A felhasználói jogosultságokat (belépés és hozzáférés) különböző intézkedésekkel biztosítják, melynek során azokat alapvetően egy meghatározott személyhez rendelik hozzá. A jogosultságok kiadása a platform-felelős dolga és azt rendszeresen ellenőrzik. A belépési jogosultságok kiadása egy meghatározott és dokumentált folyamat szerint történik. A belépési jogosultságok módosításai a négy-szem-elv alapján történik és egy verzionált log-fájlban dokumentálják.

Hozzáférési ellenőrzési, ill. -szabályozási intézkedésként különböző intézkedéseket alkalmaznak: A hozzáférési jogokat egy szerep-/ jogosultsági koncepció keretében határozzák meg és dokumentálják és a feladattól függő követelményeknek megfelelően a mindenkori szerepekhez rendelik hozzá. A technikai adminisztrátoroknak speciális szerepeket/ jogosultságokat alakítottunk ki (melyek, amennyiben technikailag lehetséges, nem teszik lehetővé a személyre vonatkozó adatokhoz való hozzáférést). A szakmai támogatásnak speciális szerepeket/ jogosultságokat alakítottunk ki (melyek, amennyiben technikailag lehetséges, nem teszik lehetővé a személyre vonatkozó adatokhoz való hozzáférést).

A szerepek/ jogosultságok meghatározása és a szerepek/ jogosultságok hozzárendelése, amennyiben technikailag és szervezés szerint lehetséges, nem ugyanaz a személy végzi és a revízióbiztos (engedélyezési) eljárásban történik és időben korlátozott. A közvetlen banki hozzáférés a szerep-/ jogosultsági koncepció megkerülésével csak a hitelesített adatbanki adminisztrátoroknak lehetséges. Létezik a magán adathordozók alkalmazására vonatkozó szabályozás, ill. a magán adathordozók alkalmazása tilos. Az adathozzáférésekre vonatkozóan kötelező szabályozások vannak érvényben a külső karbantartásokhoz, távoli karbantartásokhoz és a telefonos munkavégzéshez. A dokumentumok és adathordozók adatvédelemnek megfelelően történő megsemmisítését/ ártalmatlanítását (pl.: iratmegsemmisítő/ adatvédelmi hulladéktartály) megbízható ártalmatlanító vállalkozások végzik.

A szerep-/ jogosultsági koncepciót a változó munkaszervezési struktúrákhoz igazítják (pl.: új szerepek) és a hozzárendelt szerepeket/ jogosultságokat rendszeresen ellenőrzik (pl.: a felettes) és adott esetben hozzáigazítják, ill. megvonják. A kijelölt standardprofilokat rendszeresen központilag ellenőrzik. A változó hozzáféréseket (írás, törlés) jegyzőkönyvbe veszik és az elkészült jegyzőkönyvfájlokat alkalmas időszakra (legalább 90 nap) tárolják és (szúrópróbaszerűen) ellenőrzik.

A továbbítás biztosításának általános intézkedéseként különböző standard intézkedéseket alkalmaztak:

A továbbítással megbízott személyeket előzetesen megismertetik az elvégzendő biztonsági intézkedésekkel. A fogadói kört előre meghatározzák, úgy hogy a megfelelő ellenőrzés (hitelesítés) lehetséges legyen. Az adattovábbítás teljes folyamatát meghatározzák és dokumentálják és a konkrét adattovábbítás elvégzését jegyzőkönyvbe foglalják, ill. dokumentálják (pl.: átvételi igazolás, nyugta). A továbbítással megbízott személyek mindenekelőtt plauzibilitási, teljességi és jogossági vizsgálatokat végeznek.

A konkrét adattovábbítás elvégzése előtt megtörténik a címzett címének (pl. email-címének) ellenőrzése. Az adatok interneten való továbbítása titkosított formában történik (pl.: adattitkosítás). A továbbított adatok integritását, amennyiben technikailag lehetséges, aláírási eljárások alkalmazása biztosítja (digitális aláírás). Az elektronikus átvételi igazolást arra alkalmas formában archiválják. A nem kívánt adattovábbítást az interneten arra alkalmas technológiákkal (pl. proxy, tűzfal) letiltják.

Továbbá a különbségtétel elvégzési intézkedéseként a következő standard intézkedéseket alkalmazzák:

A különbségtétel betartására vonatkozó adatfeldolgozás célhoz kötöttségére vonatkozó szabályozás fennáll. A meghatározott célokra összegyűjtött adatokat külön tárolják a más célokra gyűjtött adatoktól. Az alkalmazott informatikai rendszerek megengedik az adatok külön tárolását (kliensképesség vagy hozzáférési koncepciók). Az adatokat a tesztelési és gyártórendszerekben is szétválasztják. Álnevesített adatoknál a kulcshidat, amely lehetővé teszi a visszaazonosíthatóságot, külön elmentik, ill. tárolják. Feldolgozási megbízásnál vagy funkcióátruházásánál a különböző Megbízók adatait külön dolgozzák fel a Megbízottnál. A meglévő szerep-/ jogosultsági koncepciók formázással lehetővé teszik a feldolgozott adatok logikus szétválasztását.

4. Az integritás biztosítása

A beírási jegyzőkönyvezés elvégzésének intézkedéseként különböző standard intézkedéseket alkalmaznak:

A hozzáférési jogok módosítását, valamint valamennyi adminisztrátori tevékenységet jegyzőkönyvbe vesznek. A beírandó hozzáférésekről (beírások, módosítások, törlések) és az adatmezők változásairól jegyzőkönyvet vesznek fel (pl.: az újonnan megadott vagy módosított adattétel tartalma). A továbbításokat (pl. letöltések) jegyzőkönyvezik és login-jegyzőkönyvezik.

A felhasznált rögzítési dokumentumokat a beírt adatok követhetőségéért dokumentálják és archiválják. A jegyzőkönyvezés tartalmazza a dátumot és a pontos időt, a felhasználót, a tevékenység fajtáját, az alkalmazási programit és az adattétel azonosítószámát. A jegyzőkönyvezés beállításait dokumentálják.

Kizárólag egy olvasói hozzáférést biztosítunk a jegyzőkönyvi adatokhoz. A jegyzőkönyvi fájlok hozzáférési jogosultjainak köre jelentősen korlátozott (pl.: ez vonatkozik az adminisztrátorra, az adatvédelmi biztosra, a revizorra). A jegyzőkönyvi fájlokat meghatározott ideig (pl. 1 év) őrzik meg és aztán az adatvédelmi szabályozásnak megfelelően törlik. Az jegyzőkönyvi fájlokat rendszeresen automatizálva kiértékelik A jegyzőkönyvi fájlok kiértékeléseit amennyiben Lehetséges álnevesített formában készítik el.

5. A rendelkezésre állás biztosítása

A felépítést belső megkettőzési mechanizmusokkal az AWS-platformon belül per se adatvesztés ellen biztosítják. Továbbá az objektumvédelmi intézkedésként az AWS következő standard intézkedéseit alkalmazzák:

Tűzvédelmi intézkedéseket végeznek el (pl.: tűzvédelmi ajtók, füstjelzők, tűzvédelmi falak, dohányzás tilalma). A számítógépek védve vannak az árvíz ellen (pl.: számítógépes helyiség az 1. emeleten, vízjelző). Intézkedéseket tesznek földrengések ellen (pl.: a számítógépes helyiséget nem teszik országutak, vasúti sínek, géphelyiségek közelébe). A számítógépeket biztosítják az elektromágneses mezők ellen (pl.: acéllemezeket tesznek a külső falakba). Intézkedéseket tesznek a vandalizmus és a lopás ellen (vesd össze a belépési ellenőrzéssel). A számítógépek klimatizált helyiségekben találhatók (a hőmérsékletet és a páratartalmat klímaberendezés szabályozza). A számítógépeket túlfeszültségi csúcsok elleni túlfeszültség-védelemmel látták el. Intézkedéseket tesznek annak biztosítása érdekében, hogy az áramellátást kevés üzemzavar szakítsa meg és folyamatos legyen az áramellátás (pl.: szünetmentes készülékek, vészhelyzeti elektromos áramfejlesztő).

Az adatállományokat rendszeresen backup-másolatokkal az AWS-platformon biztosítják. A backup-koncepciót dokumentálják és rendszeresen ellenőrzik és aktualizálják. A backup-médiát megvédik a jogosulatlan hozzáférés ellen. Az alkalmazott backup-programok megfelelnek az aktuális minőségi standardoknak és erre vonatkozóan ezeket rendszeresen aktualizálják. Berendeztek egy redundancia számítógépközpontot (az adatfeldolgozási helytől távol) és katasztrófahelyzet esetén az adatfeldolgozás ott folytatható. A rendelkezésre állási ellenőrzés különböző intézkedéseit az AWS vészhelyzetkezelési tervében dokumentálták.

Mielőtt egy adatfeldolgozási megbízást kiadnak, a Megbízottat gondosan és a meghatározott feltételek szerint (technikai és szervezési intézkedések) felülvizsgálják. Ehhez különösen a Megbízott által elvégzett technikai/ szervezési adatvédelmi intézkedések részletes bemutatását követelik meg (a kérdéskatalógus megválaszolása vagy adatvédelmi koncepció) és azokat ellenőrzik. A feldolgozott adatok mennyiségétől és érzékenységétől függően ez az ellenőrzés adott esetben helyben a Megbízottnál történik. Az arra alkalmas tanúsításokat (pl.: ISO 27001) a Megbízottak kiválasztásánál figyelembe veszik. A Megbízott alkalmasságának megállapítását méltányos és nyomon követhető formában dokumentálják.

A megbízási jogviszony megindoklásához a Megbízó és a Megbízott feldolgozási megbízási szerződést köt egymással. Ez a szerződés részletesen és írásban rögzíti a Felek illetékességeit és felelősségeit, valamint kötelezettségeit. Amennyiben egy megbízott szolgáltató a székhelyét az Európai Unión vagy az Európai Gazdasági Közösségen kívül helyezi, az Európai Unió standard szerződési záradékait alkalmazzák. Szerződésben rögzítették azt, hogy a Megbízott általi adatfeldolgozás csak a Megbízó utasításainak keretében történhet. A Megbízott köteles a Megbízó figyelmét haladéktalanul felhívni arra, ha utasításainak egyike a Megbízott véleménye szerint az adatvédelmi előírásokat megszegi. Az érintettek jogainak biztosítása érdekében, a feldolgozási megbízási szerződésben megállapodnak arról, hogy a Megbízottnak a Megbízót megfelelően támogatnia kell, amennyiben például az érintetteket értesítése szükséges.

A feldolgozási megbízási szerződés folyamán a Megbízó a Megbízott munkájának eredményeit formai szempontból és tartalmilag ellenőrzi. A Megbízottnál hozott műszaki és szervezési intézkedések betartását rendszeresen felülvizsgálják. Ehhez főként az aktuális teszteket vagy az arra alkalmas tanúsításokat, ill. az elvégzett informatikai rendszerek biztonsági vagy adatvédelmi auditjainak igazolását használják. Amennyiben alvállalkozókat vonnak be, szerződésben rögzítették azt, hogy őket megfelelően ellenőrzik.

6. A rendszerek terhelhetőségének biztosítása

A AWS-felhő infrastruktúrát a legrugalmasabb és legbiztonságosabb felhő számítógép-környezetként alakították ki. A teljes ügyfélszétválasztásnál való rendelkezésre állás optimumának megfelelően építették ki. Rendkívül fokozattal ellátható, nagyon üzembiztos platformot nyújt, amely lehetővé teszi az ügyfeleknek azt, hogy alkalmazásokat és tartalmakat szükség esetén gyorsan és biztonságosan küldjenek ki világszerte. Az AWS-szolgáltatások annyiban tartalomtól függetlenek, hogy minden ügyfélnek ugyanazt a magas biztonsági szintet nyújtják, függetlenül a tartalmak fajtájától vagy a földrajzi elhelyezkedéstől, amelyben a tartalmakat elmentették.

A magas biztonsági szintű AWS számítógépközpontok világszinten kiválóan elektronikus megfigyelő intézkedéseket alkalmaznak az aktuális műszaki szinten és több fokozatú hozzáférési ellenőrzési rendszert. A számítógépközpontokat a teljes időszakra képzett biztonsági személyzettel látják el és a hozzáférést szigorúan a legkisebb jogok elve alapján és kizárólag rendszeradminisztrációs célokra biztosítják.

7. Eljárások a személyre vonatkozó adatok rendelkezésre állásának helyreállításához fizikai vagy műszaki köztes esetben

A AWS számítógépközpontokat klaszterekben a világ különböző régióiban rendezik be. Minden számítógépközpont online és ügyfeleket szolgál ki; egy számítógépközpontot sem kapcsoltak le. Kiesés esetén az automatikus folyamatok eltolják az ügyfél-adatforgalmat az érintett területekről. A központi alkalmazásokat egy N+1 konfigurációban bocsátják rendelkezésre, úgy hogy egy számítógépközpont kiesése esetén elegendő kapacitás áll rendelkezésre, ahhoz hogy az adatforgalmat a terhelést elosztva a megmaradó telephelyek között el lehessen osztani.

Az AWS kínálja az rugalmasságot ahhoz, hogy instanciákat helyezzenek el és adatokat mentsenek el több földrajzi régión belül, valamint az egyes régiók több rendelkezésre állási zónájában. Minden rendelkezésre állási zónát független kiesési zónaként fejlesztettek ki. Ez azt jelenti, hogy az rendelkezésre állási zónákat egy jellemző városi régión belül fizikailag elosztották és például alacsony árvízveszélyt jelentő területeken találhatók (régiónként különböző árvízzóna-kategorizálás létezik). A saját szünetmentes áramellátás és a helyi vészhelyzeti áramellátás kiegészítéseképpen minden rendelkezésre állási zónát független áramszolgáltatók különböző áramhálózatain keresztül látnak el, azért hogy az egyedi hibahelyeket minimalizálni lehessen. Valamennyi rendelkezésre állási zónát redundánsan összekapcsoltak több Tier-1-tranzit-providerrel.

Az Amazon csapat az esetek kezelésére az iparágban szokásos diagnosztikai eljárásokat alkalmazza, azért hogy a vállalatot kritizáló események megszüntetését előmozdítsa. A kezelőszemélyzet folyamatosan, a nap 24 órájában, a hét hét napján és az év 365 napján szolgálatban van, hogy felismerje az üzemzavarokat és kezelje azok kihatásait és elhárítását.

8. A műszaki és szervezési intézkedések hatékonyságának rendszeres felülvizsgálati, értékelési és evolválási eljárása

A vállalkozásban meglévő irányelveket és utasításokat, ill. az információbiztonság implementált standardjait a RIO-platform bevezetésére és üzemeltetésére is használták. Az adatvédelem és az információbiztonság üzemi funkciói rendelkezésre állnak (adatvédelmi megbízott és az információbiztonsági megbízott). A foglalkoztatottakat kötelezni fogják az adattitokra és adatbiztonsági, ill. IT biztonsági intézkedésekről brosúrákkal, szórólapokkal, intranet-hivatkozással stb. tájékoztatják.

A belső folyamatokat az adatbiztonsági technikai és szervezési intézkedések betartására vonatkozóan revízióval, információbiztonságra és az adatvédelemre vonatkozóan ellenőrzik.

A feldolgozási folyamatokat és az adatbiztonsági intézkedéseket a feldolgozási tevékenységek jegyzékében dokumentálják. Az intézkedések hatékonyságát rendszeresen ellenőrzik (belső és külső ellenőrzés).