Dohoda o zpracování osobních údajů z pověření zpracovatelem

dle čl. 28 Nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů) (GDPR)

uzavřená mezi

Zákazník

- správcem – dále jen „Objednatel“ -

a společností

Wacker Neuson SE

- zpracovatelem – dále jen „Dodavatel“ -

1. Předmět a doba trvání pověření

(1) Předmět

Dodavatel zpracovává údaje uvedené v bodu 2 odst. 2 této dohody v rámci poskytování Telematických služeb pro Zákazníka (dále jen „**Osobní údaje Zákazníka**“ nebo „**Osobní údaje Zákazníků**“). Předmět pověření vyplývá z žádosti Zákazníka o zřízení účtu EquipCare u Skupiny Wacker Neuson ve spojení s Všeobecnými obchodními podmínkami (VOP) EquipCare (dále jen „**Dohoda o plnění**“).

(2) Doba trvání

Pověření trvá, dokud trvá Dohoda o plnění. Právo mimořádné výpovědi bez dodržení výpovědní doby ze závažného důvodu tím není dotčeno.

2. Konkretizace obsahu pověření

(1) Povaha a účel předvídaného zpracování Osobních údajů Zákazníků

Povaha a účel zpracování Osobních údajů Zákazníků Dodavatelem pro Objednatele spočívá v poskytování služeb v souvislosti s Telematickými službami včetně geolokace, v předávání a vyhodnocování údajů o Strojích, v prediktivní údržbě (predictive maintenance) a v udílení doporučení ohledně jednání v souvislosti s manipulací se Stroji. **Příloha 2** obsahuje podrobné pokyny Objednatele ohledně předávání Osobních údajů Zákazníků třetím stranám. Kromě toho Dodavatel z pověření Objednatele provádí anonymizaci Osobních údajů Zákazníků, které tvoří předmět této dohody. Anonymizované údaje nejsou Osobními údaji Zákazníků ve smyslu této dohody. Dodavatel je oprávněn používat tyto anonymní údaje rovněž pro vlastní účely.

Poskytování smluvně sjednaného zpracování osobních údajů je zajišťováno (i) v členské zemi Evropské unie nebo v jiném smluvním státu Dohody o Evropském hospodářském prostoru a/nebo (ii) v třetí zemi, jsou-li splněny zvláštní podmínky dle čl. 44 a násl. Obecného nařízení o ochraně osobních údajů (GDPR).

(2) Druh údajů

Předmětem zpracování Osobních údajů Zákazníků jsou tyto druhy / kategorie údajů (výčet / popis kategorií údajů)

- ☒ kmenové údaje Zákazníka (nevyužívá-li je Dodavatel jako správce osobních údajů)
- ☒ přihlašovací údaje (e-mail, heslo)
- ☒ plánovací a řídicí data
- ☒ geolokační údaje
- ☒ údaje o Strojích

(3) Kategorie subjektů údajů

Kategorie subjektů údajů dotčených zpracováním osobních údajů zahrnují:

- ☒ zaměstnance Objednatele a osob propojených ve smyslu německého zákona o akciových společnostech (AktG)
- ☐ zaměstnance Dodavatele a osob propojených ve smyslu německého zákona o akciových společnostech (AktG)
- ☐ zaměstnance Prodejních partnerů Dodavatele

3. Technicko-organizační opatření

(1) Dodavatel je povinen vést dokumentaci přijetí a provedení nezbytných technických a organizačních opatření, která byla formulována před pověřením, před zahájením zpracování, zejména ohledně konkrétního způsobu provedení příslušného pověření zpracováním.

(2) Dodavatel je povinen zabezpečit své procesy zpracování v rámci tohoto pověření dle čl. 28 odst. 3 písm. c, čl. 32 Obecného nařízení o ochraně osobních údajů (GDPR), zejména ve spojení s čl. 5 odst. 1, odst. 2 Obecného nařízení o ochraně osobních údajů (GDPR). V případě opatření, jež mají být přijata, se jedná o opatření týkající se zabezpečení údajů a zajištění úrovně ochrany přiměřené dle rizika v souvislosti se zachováním důvěrnosti, integrity, dostupnosti (disponibility) a odolnosti (zatížitelnosti) systémů. Přitom je třeba přihlédnout ke stavu techniky, k nákladům na implementaci a k povaze, rozsahu a účelům zpracování a k rozdílné míře pravděpodobnosti výskytu rizik a k různě závažným rizikům z pohledu práv a svobod fyzických osob ve smyslu čl. 32 odst. 1 Obecného nařízení o ochraně osobních údajů (GDPR). Dodavatel přijímá konkrétně opatření stanovená v **Příloze 1**.

(3) Technická a organizační opatření podléhají technickému pokroku a dalšímu vývoji. V této souvislosti je Dodavateli dovoleno provádět alternativní adekvátní opatření. Přitom však nesmí dojít ke snížení úrovně ochrany stanovených opatření. O provedených významných změnách musí být pořízena příslušná dokumentace.

4. Oprava, omezení a výmaz Osobních údajů Zákazníka

(1) Dodavatel nesmí provádět opravy, výmaz či omezovat zpracování Osobních údajů Zákazníků svévolně, ale pouze na základě zdokladovaného pokynu Objednatele. Obrátí-li se subjekt údajů v této souvislosti nebo kvůli uplatnění jiných práv subjektů údajů přímo na Dodavatele, předá Dodavatel tuto žádost Objednateli.

(2) Stanoví-li tak standardní rozsah Telematických služeb, poskytne Dodavatel Objednateli podporu/součinnost při jeho plnění práv subjektů údajů dle bodu 8 odst. 2 této dohody.

5. Zajištění kvality a jiné povinnosti Dodavatele

Dodavatel je vedle dodržení pravidel stanovených tímto pověřením povinen dodržovat povinnosti stanovené zákonem dle čl. 28 až 33 Obecného nařízení o ochraně osobních údajů (GDPR); v této souvislosti zajistí, že budou dodrženy zejména tyto požadavky:

a) Písemné jmenování pověřence pro ochranu osobních údajů, jenž svou činnost vykonává v souladu s čl. 38 a 39 Obecného nařízení o ochraně osobních údajů (GDPR). Aktuální kontaktní údaje pověřence pro ochranu osobních údajů musejí být na internetových stránkách Dodavatele vždy snadno dostupné.
b) Zachování důvěrnosti dle čl. 28 odst. 3 věta druhá písm. b, čl. 29, čl. 32 odst. 4 Obecného nařízení o ochraně osobních údajů (GDPR). Dodavatel pověří prováděním prací pouze zaměstnance, kteří jsou zavázáni k dodržování důvěrnosti a kteří byli předtím seznámeni s ustanoveními ochrany osobních údajů, jež jsou po ně relevantní. Dodavatel a každá další osoba podřízená Dodavateli, která má přístup k Osobním údajům Zákazníků, smí tyto údaje zpracovávat výhradně v souladu se zdokumentovaným pokynem Objednatele, ledaže jsou dle práva Evropské unie či členského státu EU povinni zpracovávat údaje oproti těmto pokynům. V takovém případě sdělí Dodavatel Objednateli tyto právní požadavky před zpracováním, nezakazuje-li příslušné právo takové sdělení ze závažného veřejného zájmu.
c) Objednatel a Dodavatel spolupracují na požádání s dozorovým úřadem při plnění jeho úkolů.
d) Neprodlené informování Objednatele o kontrolních úkonech a opatřeních dozorového úřadu, vztahují-li se k předmětnému pověření zpracováním. To platí i tehdy, vede-li příslušný úřad/orgán prošetřování/vyšetřování v rámci přestupkového či trestního řízení v souvislosti se zpracováním Osobních údajů Zákazníků Dodavatelem na základě jeho souvisejícího pověření ve věci zpracování osobních údajů.
e) Je-li Objednatel vystaven kontrole ze strany dozorového úřadu, přestupkovému řízení nebo trestnímu řízení, nároku některého subjektu údajů nebo třetí osoby/strany z odpovědnosti či jinému nároku v souvislosti se zpracováním osobních údajů Dodavatelem z pověření, je Dodavatel povinen poskytnout mu na základě výzvy přiměřenou podporu/součinnost.
f) Dodavatel pravidelně kontroluje interní procesy a technická a organizační opatření, aby zajistil, že zpracování v jeho oblasti odpovědnosti jako zpracovatele je v souladu s požadavky čl. 28 Obecného nařízení o ochraně osobních údajů (GDPR).
g) Prokazatelnost přijatých technických a organizačních opatření vůči Objednateli v rámci jeho kontrolních oprávnění dle bodu 7 této dohody.

6. Poddodavatelské vztahy (vztahy s dalšími zpracovateli)

(1) Poddodavatelskými vztahy ve smyslu této úpravy jsou takové služby, které poskytují „další zpracovatelé“ ve smyslu čl. 28 odst. 4 Obecného nařízení o ochraně osobních údajů (GDPR) Dodavateli jménem správce.

(2) Objednatel souhlasí s pověřením níže uvedených dalších zpracovatelů za předpokladu, že s nimi bude sjednána smluvní dohoda dle čl. 28 odst. 2-4 Obecného nařízení o ochraně osobních údajů (GDPR):

Firma dalšího zpracovatele	Země	Plnění
Amazon (AWS)	Irsko, Spojené království Velké Británie a Severního Irska, Německo	Ukládání a zpracování Osobních údajů Zákazníka „off site“
Zitcom A/S	Dánsko	Ukládání a zpracování Osobních údajů Zákazníka „on site“
OKTA Inc.	Tenant „Europe“	Řízení a správa identit
Trackunit A/S	Dánsko	Údržba a vývoj Telematických služeb
Trackunit AB	Švédsko	Údržba a vývoj Telematických služeb
Trackunit AS	Norsko	Údržba a vývoj Telematických služeb
Trackunit B.V.	Nizozemí	Údržba a vývoj Telematických služeb
Trackunit GmbH	Německo	Údržba a vývoj Telematických služeb
Trackunit Inc.	USA	Údržba a vývoj Telematických služeb
Trackunit Ltd.	Spojené království Velké Británie a Severního Irska	Údržba a vývoj Telematických služeb
Trackunit SAS	Francie	Údržba a vývoj Telematických služeb

Pověření dalších zpracovatelů nebo změna stávajícího dalšího zpracovatele je přípustná, pokud:

- Dodavatel takové pověření předem s přiměřeným časovým předstihem písemně nebo v textové podobě (formou čitelného prohlášení, v němž je uvedena osoba činící příslušný projev a které je uvedeno na datovém nosiči trvalé povahy, např. ve formě e-mailové zprávy nevyžadující vlastnoruční nebo elektronický podpis) oznámí Objednateli a
- Objednatel do 10 pracovních dnů od tohoto oznámení neuplatní vůči Dodavateli písemně nebo v textové podobě (formou čitelného prohlášení, v němž je uvedena osoba činící příslušný projev a které je uvedeno na datovém nosiči trvalé povahy, např. ve formě e-mailové zprávy nevyžadující vlastnoruční nebo elektronický podpis) z důvodu oprávněného zájmu v souvislosti s ochranou osobních údajů námitku proti zamýšlenému pověření;
- základem bude smluvní dohoda dle ustanovení čl. 28 odst. 2-4 Obecného nařízení o ochraně osobních údajů (GDPR).

Námitka Objednatele proti zamýšlené změně v souvislosti s pověřením dalšího zpracovatele nebo proti změně stávajícího dalšího zpracovatele je přípustná pouze ze závažného důvodu, jenž musí být Dodavateli prokázán. Závažný důvod je dán pouze tehdy, nelze-li změnu po Objednateli s přihlédnutím ke všem okolnostem a po zvážení oboustranných zájmů spravedlivě požadovat. Objednatel může námitku vznést pouze v přiměřené lhůtě (zpravidla dvou (2) týdnů) poté, co byl Dodavatelem informován o změně.

V případě přípustné námitky může Dodavatel vypovědět Dohodu o plnění včetně této dohody o zpracování osobních údajů z pověření zpracovatelem s účinky k okamžiku, ke kterému si Dodavatel přeje sjednat datum počátku pověření dalšího zpracovatele nebo chce provést změnu stávajícího dalšího zpracovatele a tomuto dalšímu zpracovateli chce poskytnout přístup k Osobním údajům Zákazníků. Tento okamžik uvede Dodavatel v oznámení zamýšleného pověření dalšího zpracovatele nebo změny stávajícího dalšího zpracovatele.

(3) Předání Osobních údajů Zákazníků Objednatele dalšímu zpracovateli a jeho prvotní činnost jsou dovoleny až po splnění všech podmínek pro pověření dalšího zpracovatele zpracováním.

(4) Poskytne-li další zpracovatel sjednané plnění mimo EU/EHP, zajistí Dodavatel přípustnost dle práva upravujícího oblast ochrany osobních údajů přijetím příslušných opatření. Objednatel tímto

uděluje Dodavateli oprávnění sjednávat jménem Objednatele standardní smluvní doložky EU (controller-to-processor) jako vývozce údajů („data exporter“) s případnými subdodavateli v třetích zemích mimo Evropský hospodářský prostor. Na výzvu Objednatele předloží Dodavatel Objednateli standardní smluvní doložky EU sjednané jeho jménem.

(5) Další outsourcing prostřednictvím dalšího zpracovatele (poddodavatele) vyžaduje výslovný souhlas hlavního zpracovatele (hlavního Dodavatele) (přinejmenším v textové podobě, formou čitelného prohlášení, v němž je uvedena osoba činící příslušný projev a které je uvedeno na datovém nosiči trvalé povahy, např. ve formě e-mailové zprávy nevyžadující vlastnoruční nebo elektronický podpis); veškeré smluvní úpravy obsažené v jednotlivých vzájemně navazujících smlouvách musí být sjednány i s dalším zpracovatelem (poddodavatelem).

7. Kontrolní práva Objednatele

(1) Dodavatel zajistí, aby se Objednatel mohl dle odst. (2) a (3) této dohody přesvědčit o dodržování povinností Dodavatele dle čl. 28 Obecného nařízení o ochraně osobních údajů (GDPR). Dodavatel se zavazuje, že Objednateli poskytne na základě výzvy nezbytné informace a zejména prokáže provedení technických a organizačních opatření.

(2) Prokázat přijetí takových opatření týkajících se pověření lze dle spravedlivého uvážení Dodavatele

- dodržením schválených pravidel jednání – kodexů chování dle čl. 40 Obecného nařízení o ochraně osobních údajů (GDPR);
- certifikací dle schválených postupů vydávání osvědčení dle čl. 42 Obecného nařízení o ochraně osobních údajů (GDPR);
- předložením aktuálních osvědčení, zpráv nebo výtahů ze zpráv nezávislých instancí (např. auditorů, vnitřního auditu, pověřence pro ochranu osobních údajů, IT oddělení pro zabezpečení osobních údajů, auditorů ochrany osobních údajů, auditorů pro sledování dodržení kvality);
- způsobilou certifikací provedenou, resp. způsobilým osvědčením vydaným orgánem pro bezpečnost informačních technologií nebo orgánem ochrany osobních údajů (např. dle BSI-Grundschutz, tj. v souladu se zásadami základní kybernetické ochrany stanovené německým Spolkovým úřadem pro bezpečnost informačních technologií (BSI)).

(3) Je-li Objednatel toho názoru, že doklady specifikované v odstavci (2) této dohody nejsou dostačující nebo že byla porušena tato dohoda či aplikovatelné požadavky stanovené zákonem, má Objednatel právo nechat tuto skutečnost prověřit prostřednictvím nezávislé jím pověřené třetí osoby, která je ze zákona či na základě stavovských předpisů zavázána k mlčenlivosti (dále jen „Auditor“), a to po poradě a za součinnosti s Dodavatelem, nebo prostřednictvím ověřovatelů jmenovaných v jednotlivém případě. K tomuto účelu má Objednatel právo přesvědčit se provedením namátkové kontroly, zajišťované Auditorem, která musí být včas (zpravidla dva (2) týdny před plánovanou kontrolou) ohlášena a která probíhá v obvyklých otevíracích hodinách v závodu Dodavatele, o dodržování této dohody ze strany Dodavatele. Přístup do prostor(ů) Dodavatele je možný výhradně za stálé přítomnosti zástupce Dodavatele. Tomuto zástupci náleží rozhodovací pravomoc ohledně průběhu kontroly do té míry, bude-li to nezbytné, aby se zamezilo narušení provozu Dodavatele a aby byly splněny povinnosti mlčenlivosti ze strany Dodavatele vůči třetím osobám/stranám.

(4) K podnikovým a obchodním tajemstvím Dodavatele, s nimiž se Objednatel v průběhu takové kontroly seznámí, musí Objednatel přistupovat se zachováním přísné důvěrnosti. O těchto tajemstvích nesmí být pořizovány žádné záznamy, není-li to kogentně nezbytné pro výkon kontrolního práva Objednatele.

(5) Regulérní kontroly v místě samém prováděné Objednatelem dle odstavce (3) této dohody jsou přípustné nejvýše jednou za kalendářní rok. Další kontroly ze strany Objednatele dle odstavce (3) této dohody lze provést pouze ze závažného důvodu, jenž musí být ze strany Objednatele prokázán.

(6) Za umožnění kontrol prováděných Objednatelem a za podporu/součinnost Objednatele při těchto kontrolách může Dodavatel požadovat náhradu přiměřených nákladů, jež mu v této souvislosti vzniknou, ledaže případné vady zjištěné při kontrole jsou založeny na zaviněném porušení této dohody či pokynů Objednatele Dodavatelem.

8. Povinnosti Dodavatele v oblasti poskytnutí podpory/součinnosti

(1) Dodavatel podporuje Objednatele, resp. mu poskytuje svou součinnost při dodržování povinností uvedených v čl. 32 až 36 Obecného nařízení o ochraně osobních údajů (GDPR) v oblasti zabezpečení Osobních údajů Zákazníků, v oblasti oznamovacích povinností v případě úniku dat, resp. při porušení ochrany osobních údajů, při posouzení vlivu na ochranu osobních údajů a v případě předchozích konzultací. Mezi tuto podporu/součinnost patří mj.

a) zabezpečení přiměřené úrovně ochrany přijetím technických a organizačních opatření zohledňujících okolnosti a účely zpracování a předvídanou pravděpodobnost a míru závažnosti možného porušení práva na základě mezer v oblasti zabezpečení a umožňující okamžité zjištění relevantních událostí vyvolávajících případ porušení,
b) závazek neprodleně ohlásit Objednateli porušení dostupnosti (disponibility), důvěrnosti či integrity Osobních údajů Zákazníků ve smyslu čl. 33 Obecného nařízení o ochraně osobních údajů (GDPR),
c) závazek podporovat Objednatele, resp. poskytnout mu příslušnou součinnost v rámci jeho informační povinnosti vůči subjektům údajů a poskytnout mu bez zbytečného odkladu v této souvislosti veškeré relevantní informace,
d) podpora Objednatele, resp. poskytnutí příslušné součinnosti při posouzení vlivu na ochranu osobních údajů ze strany Objednatele,
e) podpora Objednatele, resp. poskytnutí příslušné součinnosti v rámci předchozích konzultací s dozorovým úřadem.

(2) Dodavatel bude Objednatele – dle možnosti vhodnými technickými a organizačními opatřeními – v rámci toho, co po něm lze spravedlivě požadovat a co je nezbytné – podporovat ve splnění jeho povinnosti zodpovědět žádosti o hájení práv subjektu údajů ve vztahu k jeho Osobním údajům Zákazníků, týkají-li se tyto žádosti Osobních údajů Zákazníka, které tvoří předmět této dohody, zejména ohledně jeho práv dle čl. 12 až 23 Obecného nařízení o ochraně osobních údajů (GDPR).

(3) Za podpůrnou činnost, resp. součinnost, která není obsažena v popisu plnění nebo která nebyla vyvolána pochybením Dodavatele, může Dodavatel požadovat odměnu.

9. Přikazovací pravomoc Objednatele

(1) Ústní pokyny potvrdí Objednatel bez zbytečného odkladu (minimálně textovou formou, tj. formou čitelného prohlášení, v němž je uvedena osoba činící příslušný projev a které je uvedeno na datovém nosiči trvalé povahy, např. ve formě e-mailové zprávy nevyžadující vlastnoruční nebo elektronický podpis).

(2) Dodavatel je povinen informovat Objednatele bez zbytečného odkladu, je-li toho názoru, že udělený pokyn odporuje předpisům upravujícím oblast ochrany osobních údajů. Dodavatel je oprávněn přerušit provádění příslušného pokynu do doby, než bude Objednatelem potvrzen či změněn.

10. Výmaz a vrácení Osobních údajů Zákazníků

(1) Kopie či duplikáty Osobních údajů Zákazníků nebudou pořizovány bez vědomí Objednatele. Z toho jsou vyjmuty záložní kopie, jsou-li nezbytné pro zajištění řádného zpracování osobních údajů, a údaje, které jsou nezbytné s ohledem na dodržení zákonných archivačních povinností.

(2) Během doby trvání Dohody o plnění a po dobu až 10 dnů od jejího skončení umožní Dodavatel Objednateli, aby Dodavatel předal Objednateli na základě výzvy Objednatele učiněné v textové podobě (formou čitelného prohlášení, v němž je uvedena osoba činící příslušný projev a které je uvedeno na datovém nosiči trvalé povahy, např. ve formě e-mailové zprávy nevyžadující vlastnoruční nebo elektronický podpis) své Osobní údaje Zákazníků ve strojově čitelném formátu nebo aby je vymazal. Po uplynutí této lhůty Dodavatel s výhradou odstavců (3) a (4) této dohody vymaže veškeré Osobní údaje Zákazníků Objednatele nacházející se v jednotlivých službách a případné jiné Osobní údaje Zákazníků, které získal do svého držení, resp. které Dodavatel obdržel od Objednatele na základě této dohody o zpracování osobních údajů z pověření zpracovatelem, předá je Objednateli nebo je po předchozím souhlasu zničí v souladu se zákony upravujícími oblast ochrany osobních údajů. Totéž platí pro testovací materiál a vadný materiál.

(3) Shora uvedené povinnosti výmazu neplatí

(i) pro kopie Osobních údajů Zákazníků uložených na záložních médiích a/nebo záložních serverech, do jejich výmazu v souladu s uznanými postupy zabezpečení informací, přičemž Dodavatel s výhradou písm. (ii) nebude tyto uchovávané údaje a podklady/dokumenty používat k jiným účelům než k záložním účelům a ustanovení této dohody ohledně dočasného uložení se nadále použijí;

(ii) je-li Dodavatel právně zavázán k uložení Osobních údajů Zákazníků.

(4) Zničení či výmazu Osobních údajů Zákazníků je postavena na roveň anonymizace těchto údajů Dodavatelem.

(5) Dokumentace sloužící k prokázání řádného zpracování osobních údajů zpracovatelem v souladu s pověřením musí být uchovávány Dodavatelem v souladu s příslušnými archivačními lhůtami i po ukončení smlouvy/dohody. Dodavatel může pro účely splnění své povinnosti tuto dokumentaci předat ke konci uplynutí doby trvání smlouvy/dohody Objednateli.

11. Zproštění

Uplatní-li třetí osoby/strany, zejména subjekty údajů, vůči Dodavateli na základě nebo v souvislosti se zpracováním Osobních údajů Zákazníků tvořících předmět této dohody nároky vůči Dodavateli (dále jen „Nároky třetích osob“), může Dodavatel požadovat, aby Objednatel převzal obranu před těmito Nároky třetích osob a aby Dodavatele zprostil Nároků třetích osob, resp. aby mu nahradil související škodu, budou-li tyto Nároky třetích osob zjištěny na základě pravomocného rozsudku nebo budou-li Objednatelem se souhlasem Dodavatele uznány či bude-li ohledně nich ze strany Objednatele za souhlasu Dodavatele uzavřen smír. Objednatel je povinen uhradit náklady v souvislosti s obranou, resp. se smírem narovnávajícím Nároky třetích osob a nahradit Dodavateli takové náklady, resp.

náklady, které mu vznikly. Totéž platí pro náklady, které vzniknou Dodavateli přijetím případných opatření iniciovaných ze strany dozorových úřadů na základě zpracování Osobních údajů Zákazníků v rámci této dohody a pokynů Objednatele.

(2) Požaduje-li Dodavatel po Objednateli postup dle odstavce (1) této dohody, přenechá Dodavatel Objednateli ve vnitřním vztahu výhradní kontrolu nad obranou před Nároky třetích osob a poskytne Objednateli při obraně před těmito Nároky třetích osob, lze-li to po něm spravedlivě požadovat, na náklady Objednatele podporu/součinnost.

(3) Objednatel není povinen ke zproštění dle odstavce (1) této dohody, jsou-li Nároky třetích osob založeny (i) na porušení této dohody Dodavatelem nebo (ii) zvláště z anonymizace Osobních údajů Zákazníků a používání těchto anonymizovaných údajů pro účely Dodavatele.

12. Přílohy

Příloha 1: Technická a organizační opatření

Příloha 2: Specifické pokyny Objednatele ohledně předávání Osobních údajů Zákazníků třetím osobám/stranám

Příloha 1

EquipCare – Technická a organizační opatření

Tato příloha specifikuje technická a organizační opatření k zajištění bezpečného zpracování osobních údajů v rámci EquipCare dle čl. 32 Obecného nařízení o ochraně osobních údajů (GDPR). Není-li uvedeno jinak, platí opatření stejnou měrou jak pro Dodavatele Wacker Neuson, tak pro dalšího zpracovatele (poddodavatele) Trackunit. Opatření týkající se pouze jednoho ze zpracovatelů jsou příslušným způsobem označena.

Vstupní kontrola

Je zajištěna kontrola vstupu do všech prostorů, v nichž dochází ke zpracování osobních údajů.

K těmto opatřením patří:

a) Všechna důležitá zařízení jsou vybavena kontrolou vstupu.

b) Spolupracovníci/zaměstnanci mají přístupové klíče / kódy / karty.

c) Každá osoba odpovídá za zabezpečení svého klíče / své karty a jeho/její ztrátu nebo situace, které by mohly ohrozit bezpečnost budovy, oznámí ve lhůtě 24 hodin.

d) Klíče/karty nesmějí být půjčovány, rozmnožovány, pozměňovány či používány způsobem, který by umožnil vstup do prostorů nepovolaným osobám.

e) Poplachové systémy jsou aktivovány.

f) Návštěvníci a hosté se musejí zaregistrovat a jsou uvedeni v příslušném protokolu.

g) Byl vytvořen program due diligence pro všechny Zákazníky a dodavatele, včetně těch, kteří mají přístup k příslušným prostorům, jako např. úklidová služba či příslušníci ostrahy.

h) Vstupní kontroly k bezpečnostním zónám minimalizují potencionální ohrožení systémů z hlediska jejich poškození a poruch.

i) Přístup k prostorům, v nichž jsou umístěny servery / komunikační zařízení je omezen na autorizovaný personál.

j) Fyzické datové nosiče jsou uschovávány v uzamčených skříních.

Přístup k systému

Přístup k systémům zpracovávajícím osobní údaje, resp. k IT systémům mají umožněn pouze autorizovaní a ověření (autentizovaní) uživatelé.

K těmto opatřením patří:

a) Uživatelé služeb jsou vždy ověřováni na základě jednoznačných uživatelských jmen a hesel.

b) Přístup je zajištěn použitím VPN a příp. MFA (vícefaktorovou autentizací).

c) Dálkový přístup k systémům není třetím osobám/stranám nikdy povolen, ledaže byl výslovně schválen. V případě poskytnutí takového přístupu je tento přístup vždy monitorován.

d) Poskytnuté služby jsou zabezpečeny prostřednictvím firewallů a neautorizovaný externí přístup k nim je blokován šifrováním.

e) Služby provozované ze strany Trackunit jsou nepřetržitě monitorovány nástroji zajišťujícími kontinuální skenování slabých a zranitelných míst tak, aby byla zajištěna maximální míra zabezpečení.

f) Servery a počítačová pracoviště jsou kontinuálně updatovány v souladu s kybernetickou bezpečností chránící před zneužitím slabých a zranitelných míst v používaných aplikacích.

g) Trackunit převedla osobní údaje (úplné jméno, uživatelské jméno, heslo, e-mail apod.) novému providerovi spravujícímu identity (Identity Management Provider). Tato migrace zajistí, že osobní údaje jsou zcela zašifrovány a uloženy u vysoce moderního poskytovatele správy identit (okta.com) certifikovaného dle SOC 2 typ 1 a 2, ISO 27001, ISO 27018 a CSA Star Level 2.

h) Osoby, které mají oprávnění k přístupu k chráněným částem IT systémů, obdrží od IT administrátorů zvláštní heslo. Heslo musí být pravidelně měněno a musí splňovat definované minimální požadavky ohledně jeho délky a komplexity.

i) Počítače a jiné přístroje musejí být používány v souladu s interními směrnicemi. Přístroje tak musejí být např. při opouštění prostorů zablokovány (clear screen policy).

j) Na straně Trackunit se všichni vývojáři účastní povinného školení v oblasti kybernetické bezpečnosti.

Přístup k datům

Osoby oprávněné používat systémy zpracovávající data, resp. IT systémy mají přístup pouze k osobním údajům, pro které jsou autorizovány.

K těmto opatřením patří:

a) Pracovníci/zaměstnanci oprávnění zpracovávat osobní údaje byli zavázáni zachovávat mlčenlivost nebo jsou příslušným zákonem zavázáni dodržováním povinnosti mlčenlivosti.

b) Přístup pracovníků/zaměstnanců k výrobním systémům, vývojářskému prostředí a službám je omezen na osoby, které jsou pro plnění příslušných pracovních úkolů nezbytné.

c) Přístup bude povinně modifikován či zrušen, pokud příslušná osoba změní pracovní pozici či zaměstnavatele.

d) Interní oddělení IT provádí pravidelné prověrky, aby zajistilo, že všechna poskytnutá práva odpovídají pracovnímu zařazení jednotlivých pracovníků/zaměstnanců.

e) Přístup ke zdrojům IT není umožněn nikomu, kdo není proškolen či jinak přiměřeně poučen o svých úkolech v oblasti zabezpečení osobních údajů / kybernetické bezpečnosti.

Předání údajů

Osobní údaje jsou chráněny před čtením, kopírováním, pozměněním či výmazem ze strany nepovolaných osob během přenosu dat.

K těmto opatřením patří:

a) Trackunit RAW používá standard pokročilého šifrování (advanced encryption standard (AES)).

b) Trackunit IRIS zasílá zašifrované mikroprogramové vybavení (firmware) společně s bezpečným hash algoritmem pro ověření autentizace a integrity příslušným přístrojům.

c) Komunikace mezi službami (Manager, Go, On) a IRIS je implementována jako rozhraní REST se šifrováním HTTPS.

d) Veřejné Trackunit-API používá šifrování HTTPS.

e) Komunikace mezi Trackunit RAW a IRIS je založena na síti GSM a chráněna šifrováním GSM. Pro datovou komunikaci je používán vlastní protokol na IP/UDP. SMS jsou příležitostně používány pro správu přístrojů.

f) Komunikace přijatá přístroji RAW je vždy validována různými prostředky tak, aby bylo zajištěno, že přístroje akceptují pouze autorizované dotazy.

g) Kromě šifrování GSM zavede společnost Trackunit šifrování end-to-end komunikace m2m mezi příslušným přístrojem a cloudem.

Integrita a dostupnost

Tato opatření zajišťují, že osobní údaje zůstanou během zpracování úplné a správné a garantují, že osobní údaje jsou chráněny před neúmyslným zničením či ztrátou a že v případě incidentu / porušení zabezpečení osobních údajů dojde k včasnému obnovení či dostupnosti osobních údajů.

K těmto opatřením patří:

a) Databáze jsou denně zabezpečovány tak, aby bylo umožněno obnovení systémů v případě poruchy.

b) Společnost Trackunit implementovala proces řízení incidentů (případů porušení zabezpečení osobních údajů) s nepřetržitým monitorováním kritických služeb.

c) Společnost Trackunit vypracovala plán reakce na incidenty (IR plán) (případy porušení zabezpečení osobních údajů), který musí být v případě vzniku incidentu dodržen. Tento plán definuje jednotlivé přiřazené oblasti odpovědnosti a zahrnuje harmonogram vypracovaný pro dotčené osoby tak, aby byly splněny lhůty pro oznámení stanovené Obecným nařízením o ochraně osobních údajů (GDPR). Tento plán reakce na incidenty (IR plán) (případy porušení zabezpečení osobních údajů) zahrnuje rovněž externí komunikaci.

e) Lhůty pro výmaz a archivaci se řídí platným právem.

Dohody o zpracování osobních údajů z pověření zpracovatelem

Osobní údaje zpracovávané z pověření Zákazníka jsou zpracovávány výhradně v souladu s příslušnou dohodou a příslušnými pokyny Zákazníka. Se všemi společnostmi, které mohou mít přístup k osobním údajům, budou uzavřeny dohody o zpracování osobních údajů z pověření zpracovatelem dle čl. 28 Obecného nařízení o ochraně osobních údajů (GDPR).

Separace dat

Osobní údaje shromažďované pro různé účely budou zpracovávány odděleně.

K těmto opatřením patří:

a) Osobní údaje získané z přístrojů/Strojů jsou automaticky přiřazovány různým Zákazníkům. Údaje jsou vždy odděleny od Zákazníků.

b) Zákazník má přístup pouze ke svým vlastním osobním údajům.

c) K osobním údajům Zákazníků je vždy přistupováno se zachováním mlčenlivosti a důvěrnosti. Auditní práva, která byla případně Zákazníkům poskytnuta, vždy vylučují právo či možnost nahlížet do údajů jiných Zákazníků.

Compliance – dodržování právních a etických norem

Byly vytvořeny procesy pravidelné kontroly, vyhodnocování a hodnocení účinnosti technických a organizačních opatření pro zajištění zabezpečení zpracování osobních údajů.

a) Společnost Wacker Neuson SE jmenovala pověřence pro ochranu osobních údajů, který je prostřednictvím e-mailové adresy datenschutz@wackerneuson.com k dispozici pro otázky a záležitosti související se zpracováním osobních údajů. Společnost Trackunit rovněž jmenovala pověřence pro ochranu osobních údajů.

b) Vytyčené zásady a směrnice týkající se ochrany osobních údajů jsou každoročně přezkoumávány a příp. aktualizovány.

c) Je k dispozici posouzení vlivu na ochranu osobních údajů tak, aby bylo možné provést vyhodnocení dopadů zpracování na ochranu osobních údajů dle čl. 35 Obecného nařízení o ochraně osobních údajů (GDPR).

d) Jsou činěny přiměřené kroky zajišťující, že personál je seznámen s technickými a organizačními opatřeními specifikovanými v tomto dokumentu a že je dodržuje. Všichni pracovníci/zaměstnanci musejí v přiměřených intervalech absolvovat školení zajišťovaná pověřencem pro ochranu osobních údajů.

e) Společnost Trackunit realizuje v zájmu identifikace rizik každý druhý týden program due diligence ve vztahu ke všem Zákazníkům a dodavatelům.

Příloha 2

Specifické pokyny Objednatele ohledně předání Osobních údajů Zákazníků třetím osobám/stranám

Dle Dohody o plnění umožňuje Telematické řešení Přístup k Osobním údajům Zákazníků ze strany Dodavatele, jiných společností náležejících do Skupiny Wacker Neuson a Prodejních partnerů Dodavatele vždy k vlastním obchodním účelům (např. poskytování Služeb EquipCare na vyžádání Objednatele nebo pro účely vývoje výrobků).

Níže uvedení příjemci mají mít konkrétně přístup k Osobním údajům Zákazníků pro tyto vlastní obchodní účely:

Příjemce	**Příslušný vlastní obchodní účel**
Wacker Neuson SE	• Podpora L2 (druhého stupně) (na základě konkrétní žádosti Objednatele o poskytnutí podpory)
Výrobní společnost (Skupiny Wacker Neuson), která vyrobila příslušný Stroj, z něhož byly příslušné Osobní údaje Zákazníků předány.	• Podpora L2 (druhého stupně) (na základě konkrétní žádosti Objednatele o poskytnutí podpory) • Vývoj produktů • Přezkoumání případných nároků ze záruky či garance
Prodejní společnost (Skupiny Wacker Neuson), která prodala příslušný Stroj, z něhož byly předány příslušné Osobní údaje Zákazníků, přímo Objednateli, případnému předchozímu držiteli nebo jinak zprostředkovateli.	• Podpora L1 (prvního stupně) (first level support) (na základě konkrétní žádosti Objednatele o poskytnutí podpory) • Přezkoumání případných nároků ze záruky či garance
Obchodník (Prodejní partner), který prodal příslušný Stroj, z něhož byly předány příslušné Osobní údaje Zákazníků, Objednateli nebo případnému předchozímu držiteli.	• Podpora L1 (prvního stupně) (first level support) (na základě konkrétní žádosti Objednatele o poskytnutí podpory) • Přezkoumání případných nároků ze záruky či garance

Objednatel tímto uděluje Dodavateli pokyn předávat Osobní údaje Zákazníků poskytnutím přístupových práv shora uvedeným příjemcům k účelům, jež jsou shora uvedeny, je-li to nezbytné pro příslušné shora uvedené vlastní obchodní účely těchto příjemců. V této souvislosti jednají tito příjemci vždy jako správci ve smyslu čl. 4 odst. 7 Obecného nařízení o ochraně osobních údajů (GDPR).

Je-li Dodavatel sám příjemcem příslušných Osobních údajů Zákazníků, zavazuje se Dodavatel tímto vůči Objednateli, že bude zpracovávat Osobní údaje Zákazníků výhradně ke shora uvedeným účelům a že v co možná nejlepší míře zamezí vytvoření přímé osobní vazby k těmto údajům. Dodavatel se rovněž zavazuje, že nebude vytvářet kopie Osobních údajů Zákazníků, ale že bude Osobní údaje Zákazníků zpracovávat výhradně na Portálu provozovaném Dodavatelem (dle definice Dohody o plnění). To nezahrnuje vytváření kopií anonymizovaných informací.