Porozumienie w sprawie powierzenia przetwarzania danych

zgodnie z art. 28 RODO

pomiędzy

Klient

- Administratorem – zwanym dalej Powierzającym -

a

Wacker Neuson Se

- Podmiotem Przetwarzającym – zwanym dalej Wykonawcą -

1. Przedmiot i czas trwania zlecenia

(1) Przedmiot

Wykonawca przetwarza określone w punkcie 2 ust. 2 niniejszego porozumienia dane (zwane dalej „**Danymi Osobowymi Klienta**“) w ramach wykonywania Usług Telematycznych dla Klienta. Przedmiot zlecenia wynika z wniosku Klienta o utworzenie konta w ramach Wacker Neuson Group EquipCare w związku z obowiązywaniem Ogólnych Warunków Handlowych EquipCare (zwanego dalej „**Porozumieniem W Sprawie Świadczenia**“).

(2) Czas trwania

Zlecenie jest wiążące przez okres obowiązywania Porozumienia W Sprawie Świadczenia. Powyższe nie narusza prawa wypowiedzenia w trybie nadzwyczajnym z ważnej przyczyny.

2. Szczegółowa treść zlecenia

(1) Sposób i cel przewidywanego przetwarzania Danych Osobowych Klienta

Sposobem i celem przetwarzania Danych Osobowych Klienta przez Wykonawcę na rzecz Powierzającego jest świadczenie usług w związku z Usługami Telematycznymi, w tym geolokalizacja, konserwacja zapobiegawcza (Predictive Maintenance) oraz wskazówki dotyczące obsługi maszyn. **Załącznik nr 2** zawiera szczegółowe instrukcje Powierzającego dotyczące przekazywania Danych Osobowych Klienta podmiotom trzecim. Ponadto Wykonawca na wniosek Powierzającego anonimizuje Dane Osobowe Klienta będące przedmiotem niniejszego porozumienia. Zanonimizowane dane nie stanowią Danych Osobowych Klienta w rozumieniu niniejszego porozumienia. Wykonawca jest uprawniony do korzystania z tych anonimowych danych także do własnych celów.

Przetwarzanie danych na podstawie niniejszego porozumienia odbywa się (i) w państwie członkowskim Unii Europejskiej lub w innym państwie-stronie Porozumienia o Europejskim Obszarze

Gospodarczym i/lub (ii) w państwie trzecim, jeżeli spełnione są warunki szczególne określone w art. 44 i nast. RODO.

(2) Rodzaj danych

Przedmiotem przetwarzania Danych Osobowych Klienta są następujące rodzaje/kategorie danych (lista/opis kategorii danych):

- ☒ dane statyczne Klienta (o ile Wykonawca nie wykorzystuje ich jako administrator)
- ☒ dane do logowania (E-mail, hasło)
- ☒ dane dot. planowania i dane sterujące
- ☒ dane dot. geolokalizacji
- ☒ dane dot. maszyn

(3) Kategorie osób, których dane dotyczą

Kategorie osób objętych przetwarzaniem:

- ☒ pracownicy Powierzającego i jego jednostek powiązanych w rozumieniu niem. ustawy o spółkach akcyjnych
- ☐ pracownicy Wykonawcy i jego jednostek powiązanych w rozumieniu niem. ustawy o spółkach akcyjnych
- ☐ pracownicy dystrybutorów Wykonawcy

3. Środki techniczne i organizacyjne

(1) Przed rozpoczęciem przetwarzania Wykonawca zobowiązany jest udokumentować wykonanie czynności, jakie przed udzieleniem zlecenia zostały mu przedstawione jako środki techniczne i organizacyjne, konieczne w szczególności dla realizacji tego konkretnego zlecenia.

(2) Wykonawca ma obowiązek zapewnienia bezpieczeństwa realizowanych w ramach niniejszego zlecenia procesów przetwarzania zgodnie z art. 28 ust. 3 lit. c, art. 32 RODO, w szczególności w związku z art. 5 ust. 1 i ust. 2 RODO. Działania, jakie powinny zostać podjęte, dotyczą co do zasady bezpieczeństwa danych oraz zapewnienia odpowiadającego ryzyku stopnia ochrony poufności, integralności, dostępności i odporności systemów przetwarzania. Uwzględniać przy tym należy stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia w rozumieniu art. 32 ust. 1 RODO. Konkretne działania, które powinien podjąć Wykonawca, określa **Załącznik nr 1**.

(3) Środki techniczne i organizacyjne podlegają postępowi technicznemu i rozwojowi. Dlatego Wykonawcy zezwala się na wprowadzanie adekwatnych alternatywnych rozwiązań. Nie może zostać przy tym obniżony poziom bezpieczeństwa ustalonych działań. Istotne zmiany muszą być dokumentowane.

4. Poprawianie, ograniczanie przetwarzania i usuwanie Danych Osobowych Klienta

(1) Wykonawca może nie samodzielnie, lecz zgodnie z udokumentowanym poleceniem Powierzającego poprawiać, usuwać Dane Osobowe Klienta bądź ograniczać ich przetwarzanie. Jeżeli osoba, której dane dotyczą, zwróci się w związku z tym lub w celu dochodzenia innych praw osoby, której dane dotyczą, bezpośrednio do Wykonawcy, Wykonawca przekaże taki wniosek Powierzającemu.

(2) O ile jest to objęte standardowym zakresem Usług Telematycznych, Wykonawca wspiera Powierzającego przy wykonywaniu przez niego praw osób, których dane dotyczą, zgodnie z punktem 8 ust. 2 niniejszego porozumienia.

5. Zapewnienie jakości i inne obowiązki Wykonawcy

Wykonawca poza przestrzeganiem regulacji niniejszego zlecenia ma obowiązek wypełniania obowiązków ustawowych wynikających z art. 28–33 RODO; w związku z tym gwarantuje on w szczególności przestrzeganie następujących wymogów:

a) Pisemne wyznaczenie inspektora ochrony danych, który swoje zadania wypełnia zgodnie z art. 38 i 39 RODO. Jego dane kontaktowe publikowane są w łatwo dostępnej formie na stronie internetowej Wykonawcy.
b) Zachowanie poufności zgodnie z art. 28 ust. 3 zdanie drugie lit. b, art. 29, art. 32 ust. 4 RODO. Wykonawca zatrudnia do realizacji prac wyłącznie osoby zobowiązane do zachowania poufności i zaznajomione wcześniej z dotyczącymi ich przepisami w zakresie ochrony danych. Wykonawca oraz każda podporządkowana Wykonawcy osoba, mająca dostęp do Danych Osobowych Klienta, mogą przetwarzać te dane wyłącznie zgodnie z udokumentowanym poleceniem Powierzającego, chyba że zgodnie z prawem unijnym lub prawem jednego z krajów członkowskich UE zobowiązani są do przetwarzania danych w sposób sprzeczny z takimi poleceniami. W takim przypadku Wykonawca powiadamia Powierzającego o powyższych wymogach prawnych przed przystąpieniem do przetwarzania danych, o ile właściwe prawo z uwagi na ważny interes publiczny nie zabrania takiego powiadomienia.
c) Współpraca Powierzającego i Wykonawcy na wniosek organu nadzorczego przy prowadzeniu jego działań.
d) Niezwłoczne powiadomienie Powierzającego o działaniach kontrolnych organu nadzorczego, o ile dotyczą one zakresu niniejszego zlecenia. Powyższe dotyczy także sytuacji, gdy właściwy organ prowadzi u Wykonawcy dochodzenie w postępowaniu o wykroczenie lub postępowaniu karnym dotyczącym przetwarzania powierzonych Danych Osobowych Klienta.
e) W przypadku gdy to Powierzający objęty jest kontrolą organu nadzorczego, postępowaniem o wykroczenie lub postępowaniem karnym, roszczeniem odszkodowawczym osoby, której dane dotyczą, lub osoby trzeciej bądź innym roszczeniem w związku z przetwarzaniem danych powierzonych u Wykonawcy, Wykonawca na żądanie udziela Powierzającemu stosownego wsparcia.
f) Wykonawca regularnie kontroluje swoje procedury wewnętrzne oraz środki techniczne i organizacyjne, aby zagwarantować przetwarzanie danych w ramach jego odpowiedzialności jako podmiotu przetwarzającego zgodnie z wymogami art. 28 RODO.
g) Dokumentowanie podejmowanych środków technicznych i organizacyjnych wobec Powierzającego w ramach uprawnień kontrolnych Powierzającego wynikających z punktu 7 niniejszego porozumienia.

6. Stosunek podwykonawstwa

(1) Za stosunek podwykonawstwa w rozumieniu niniejszej regulacji uważa się usługi świadczone w imieniu Administratora na rzecz Wykonawcy przez „inne podmioty przetwarzające” w rozumieniu art. 28 ust. 4 RODO.

(2) Powierzający wyraża zgodę na zatrudnienie poniższych podwykonawców pod warunkiem zawarcia umowy zgodnie z postanowieniami art. 28 ust. 2-4 RODO:

Firma podwykonawcy	Kraj	Świadczenie
Amazon (AWS)	Irlandia, Wlk. Brytania, Niemcy	„pozamiejscowe" przechowywanie i przetwarzanie Danych Osobowych Klienta
Zitcom A/S	Dania	przechowywanie i przetwarzanie Danych Osobowych Klienta „na miejscu"
OKTA Inc.	Tenant „Europe"	Zarządzanie tożsamością
Trackunit A/S	Dania	konserwacja i rozwój Usług Telematycznych
Trackunit AB	Szwecja	konserwacja i rozwój Usług Telematycznych
Trackunit AS	Norwegia	konserwacja i rozwój Usług Telematycznych
Trackunit B.V.	Holandia	konserwacja i rozwój Usług Telematycznych
Trackunit GmbH	Niemcy	konserwacja i rozwój Usług Telematycznych
Trackunit Inc.	USA	konserwacja i rozwój Usług Telematycznych
Trackunit Ltd.	Wlk. Brytania	konserwacja i rozwój Usług Telematycznych
Trackunit SAS	Francja	konserwacja i rozwój Usług Telematycznych

Zatrudnianie dalszych podwykonawców lub zmiana aktualnego podwykonawcy jest dopuszczalna, jeżeli:

- Wykonawca zgłosi takie zlecenie Powierzającemu z odpowiednim wyprzedzeniem na piśmie bądź w formacie tekstowym oraz
- Powierzający w terminie 10 dni roboczych po dokonaniu takiego zgłoszenia nie wniesie w formie pisemnej bądź tekstowej sprzeciwu wobec planowanego zlecenia z uwagi na uzasadniony interes z punktu widzenia ochrony danych;
- podstawę stanowić będzie umowa sporządzona zgodnie z postanowieniami art. 28 ust. 2-4 RODO.

Sprzeciw Powierzającego wobec planowanego zatrudnienia dalszego podwykonawcy lub zmiany aktualnego podwykonawcy dopuszczalny jest wyłącznie z ważnej przyczyny, udokumentowanej wobec Wykonawcy. Ważna przyczyna zachodzi jedynie wówczas, gdy zmiana po uwzględnieniu wszystkich okoliczności i rozważeniu obopólnych interesów jest dla Powierzającego nie do przyjęcia. Powierzający może wnieść sprzeciw jedynie w stosownym terminie (zasadniczo dwóch (2) tygodni) po powiadomieniu przez Wykonawcę o zmianie.

W przypadku wniesienia dopuszczalnego sprzeciwu Wykonawca może wypowiedzieć Porozumienie W Sprawie Świadczenia, z niniejszym porozumieniem w sprawie powierzenia przetwarzania danych włącznie, ze skutkiem na dzień, z którym Wykonawca zamierza zatrudnić dalszego podwykonawcę wzgl. rozpocząć zmianę aktualnego podwykonawcy i umożliwić temu podwykonawcy dostęp do Danych Osobowych Klienta. Powyższy termin Wykonawca wskazuje w zgłoszeniu planowanego zatrudnienia dalszego podwykonawcy wzgl. zmiany aktualnego podwykonawcy.

(3) Przekazanie podwykonawcy Danych Osobowych Klienta Powierzającego i przystąpienie do wykonywania czynności przez podwykonawcę możliwe jest dopiero po spełnieniu wszystkich warunków dla jego zatrudnienia.

(4) Jeżeli podwykonawca wykonuje uzgodnione świadczenie poza terytorium UE/EOG, Wykonawca podejmując stosowne środki zapewnia jego dopuszczalność w świetle ochrony danych. Powierzający niniejszym udziela Wykonawcy uprawnienia do zawierania w imieniu Powierzającego standardowych klauzul umownych UE (controller-to-processor) w charakterze „przekazującego dane" z ewentualnymi podwykonawcami w krajach trzecich poza Europejskim Obszarem Gospodarczym. Na żądanie Powierzającego Wykonawca przedkłada Powierzającemu zawarte w jego imieniu standardowe klauzule umowne UE.

(5) Dalsze przekazywanie danych przez podwykonawcę wymaga wyraźnej zgody głównego Wykonawcy (co najmniej w formacie tekstowym); wszelkie regulacje umowne w łańcuchu kontraktowym powinny być nakładane także na każdego kolejnego podwykonawcę.

7. Prawa kontrolne Powierzającego

(1) Wykonawca zapewnia Powierzającemu możliwość kontroli wykonywania przez Wykonawcę obowiązków określonych w art. 28 RODO zgodnie z postanowieniami ust. 2 i 3. Wykonawca zobowiązuje się udzielać Powierzającemu na jego żądanie koniecznych informacji, a w szczególności dokumentować realizację środków technicznych i organizacyjnych.

(2) Udokumentowanie podjęcia środków dotyczących zlecenia przez Wykonawcę może nastąpić na zasadzie słuszności poprzez

- przestrzeganie kodeksów postępowania zgodnie z art. 40 RODO;
- certyfikację w ramach zatwierdzonego postępowania certyfikacyjnego zgodnie z art. 42 RODO;
- aktualne poświadczenia, sprawozdania lub wyciągi ze sprawozdań niezależnych instancji (np. biegłego rewidenta, jednostki rewizyjnej, inspektora ochrony danych, działu bezpieczeństwa IT, audytorów ochrony danych, audytorów jakościowych);
- stosowną certyfikację w ramach audytu bezpieczeństwa informatycznego lub audytu ochrony danych (np. zgodnie z BSI-IT Grundschutz – podstawowymi zasadami ochrony informatycznej wydanymi przez niem. Federalny Urząd ds. Bezpieczeństwa Techniki Informatycznej).

(3) Jeżeli w opinii Powierzającego dowody opisane w ust. 2 są niewystarczające bądź miało miejsce naruszenie niniejszego porozumienia lub obowiązujących wymogów ustawowych, Powierzającemu przysługuje prawo zlecenia przeprowadzenia w porozumieniu z Wykonawcą kontroli przez wyznaczony przez niego niezależny i zobowiązany ustawowo lub w ramach standardów zawodowych do zachowania poufności podmiot trzeci („Audytora") lub też przez wyznaczone w indywidualnych przypadkach osoby kontrolujące. W tym celu Powierzający ma prawo sprawdzania przestrzegania niniejszego porozumienia przez Wykonawcę w drodze – prowadzonych przez Audytora – wyrywkowych kontroli, o których należy powiadomić z wyprzedzeniem czasowym (co do zasady dwa (2) tygodnie przed planowaną kontrolą), w zwykłych godzinach pracy w przedsiębiorstwie Wykonawcy. Wstęp do pomieszczeń Wykonawcy odbywa się wyłącznie przy stałej obecności przedstawiciela Wykonawcy. Przedstawiciel ten ma moc decydującą o przebiegu kontroli w zakresie, jaki jest konieczny dla uniknięcia zakłóceń w pracy przedsiębiorstwa Wykonawcy oraz zapewnienia wykonania obowiązku zachowania przez Wykonawcę tajemnicy wobec osób trzecich.

(4) Tajemnice przedsiębiorstwa i tajemnice handlowe Wykonawcy, które staną się podczas takiej kontroli znane Powierzającemu, Powierzający powinien traktować z najwyższą poufnością. Nie wolno

sporządzać w ich zakresie zapisów, o ile nie jest to absolutnie konieczne dla celów wykonywania przez Powierzającego jego prawa kontroli.

(5) Dokonywanie przez Powierzającego regularnych kontroli na miejscu zgodnie z ustępem 3 dopuszczalne jest maksymalnie raz w roku kalendarzowym. Dodatkowe kontrole ze strony Powierzającego zgodnie z ustępem 3 mogą być prowadzone wyłącznie z ważnej, udokumentowanej przez Powierzającego przyczyny.

(6) W celu umożliwienia Powierzającemu kontroli oraz udzielania mu wsparcia podczas takich kontroli Wykonawca może żądać zwrotu poniesionych w związku z tym przez niego kosztów w stosownym wymiarze, chyba że ewentualnie stwierdzone podczas kontroli uchybienia wynikają z zawinionego działania Wykonawcy wbrew niniejszemu porozumieniu lub poleceniom Powierzającego.

8. Obowiązki Wykonawcy w zakresie zapewnienia wsparcia

(1) Wykonawca wspiera Powierzającego przy wypełnianiu obowiązków wynikających z art. 32–36 RODO w zakresie bezpieczeństwa Danych Osobowych Klienta, zgłaszania nadużyć danych, oceny skutków dla ochrony danych oraz uprzednich konsultacji. Należą do nich m.in.

a) zapewnienie właściwego stopnia ochrony danych przy pomocy środków technicznych i organizacyjnych, które uwzględniają okoliczności i cele przetwarzania oraz prognozowane prawdopodobieństwo i ciężar możliwego naruszenia prawa na skutek luk w ochronie, a także umożliwiają natychmiastową identyfikację relewantnych przypadków naruszeń,
b) obowiązek niezwłocznego zgłaszania Powierzającemu naruszeń dostępności, poufności lub integralności Danych Osobowych Klienta w rozumieniu art. 33 RODO,
c) obowiązek wspierania Powierzającego przy wypełnianiu jego obowiązków informacyjnych wobec osób, których dane dotyczą, i niezwłocznego udostępniania im wszelkich stosownych informacji,
d) wspieranie Powierzającego przy ocenie skutków przetwarzania dla ochrony danych osobowych,
e) wspieranie Powierzającego w ramach uprzednich konsultacji z organem nadzorczym.

(2) Wykonawca będzie wspierał Powierzającego – zgodnie ze swoimi możliwościami, odpowiednimi środkami technicznymi i organizacyjnymi – w dopuszczalnych granicach i stosownie do konieczności przy wypełnianiu obowiązku rozpatrywania wniosków o dochodzenie praw osób, których dane dotyczą, w stosunku do ich Danych Osobowych Klienta, o ile takie wnioski dotyczą Danych Osobowych Klienta objętych niniejszym porozumieniem, w szczególności w odniesieniu do ich praw wynikających z art. 12–23 RODO.

(3) Z tytułu działań wspierających, wychodzących poza zakres opisu świadczenia lub niemających źródła w niewłaściwym postępowaniu Wykonawcy, Wykonawca może żądać wynagrodzenia.

9. Prawo Powierzającego do wydawania poleceń

(1) Polecenia ustne potwierdzane są przez Powierzającego niezwłocznie (co najmniej w formie tekstowej).

(2) Wykonawca ma obowiązek niezwłocznego poinformowania Powierzającego, jeżeli jego zdaniem któreś z poleceń stanowi naruszenie przepisów o ochronie danych osobowych. Wykonawca jest uprawniony do niewykonywania polecenia do czasu gdy zostanie ono przez Powierzającego potwierdzone lub zmienione.

10. Usuwanie lub zwrot Danych Osobowych Klienta

(1) Kopie lub duplikaty Danych Osobowych Klienta nie są sporządzane bez wiedzy Powierzającego. Wyjątek stanowią kopie bezpieczeństwa, o ile są potrzebne dla zapewnienia prawidłowego

przetwarzania danych, oraz dane konieczne z punktu widzenia wypełniania ustawowych obowiązków przechowywania.

(2) Przez okres obowiązywania Porozumienia W Sprawie Świadczenia oraz przez okres do 10 dni po jego zakończeniu Wykonawca stworzy dla Powierzającego możliwość, aby na wyrażone w formie tekstowej żądanie Powierzającego Wykonawca przekazał Powierzającemu jego Dane Osobowe Klienta w formacie umożliwiającym ich przetwarzanie bądź je usunął. Po upływie tego terminu Wykonawca, z zastrzeżeniem ustępów 3 i 4, usunie wszelkie Dane Osobowe Klienta Powierzającego zawarte w zasobach Usług Telematycznych, a ewentualne inne Dane Osobowe Klienta, które weszły w posiadanie Wykonawcy, a które Wykonawca na podstawie niniejszego porozumienia otrzymał od Powierzającego do przetwarzania na jego zlecenie, zostaną Powierzającemu zwrócone bądź po uprzednim wyrażeniu zgody zniszczone zgodnie z przepisami o ochronie danych. Powyższe dotyczy także materiałów testowych i wybrakowanych.

(3) Powyższe obowiązki w zakresie usuwania danych nie obowiązują

(i) dla kopii Danych Osobowych Klienta, zapisanych na nośnikach kopii bezpieczeństwa i/lub na serwerach zapasowych, do chwili ich planowanego usunięcia zgodnie z uznanymi procedurami bezpieczeństwa informatycznego, przy czym Wykonawca z zastrzeżeniem lit. (ii) nie będzie wykorzystywał takich przechowywanych danych i dokumentacji do żadnych innych celów niż tworzenie kopii bezpieczeństwa, a postanowienia niniejszej umowy dotyczące powyższego czasowego przechowywania będą miały nadal zastosowanie;

(ii) w przypadkach, w których Wykonawca ma ustawowy obowiązek przechowywania Danych Osobowych Klienta.

(4) Równoznaczna ze zniszczeniem lub usunięciem Danych Osobowych Klienta jest anonimizacja tych danych przez Wykonawcę.

(5) Dokumentacje, służące potwierdzaniu przetwarzania danych w sposób prawidłowy i zgodny ze zleceniem, Wykonawca ma obowiązek przechowywać zgodnie ze stosownymi terminami przechowywania po zakończeniu umowy. W celu odciążenia siebie Wykonawca może je z chwilą zakończenia umowy przekazać Powierzającemu.

11. Zwolnienie

(1) W przypadku zgłaszania przez osoby trzecie, w szczególności osoby, których dane dotyczą, roszczeń wobec Wykonawcy na podstawie lub w związku z przetwarzaniem Danych Osobowych Klienta, stanowiących przedmiot niniejszej umowy („Roszczenia Osób Trzecich“), Wykonawca może zażądać, aby Powierzający przyjął odpieranie Roszczeń Osób Trzecich na siebie i zwolnił z nich Wykonawcę, o ile roszczenia te potwierdzono prawomocnym orzeczeniem lub mogą one za zgodą Wykonawcy być przedmiotem ugody lub zostać przez Powierzającego uznane. Powierzający ponosi koszty związane z odpieraniem Roszczeń Osób Trzecich bądź ich regulacją w drodze ugody i zobowiązany jest zwrócić Wykonawcy ewentualnie powstałe po jego stronie koszty tego rodzaju. Powyższe dotyczy wszelkich kosztów ponoszonych przez Wykonawcę z tytułu ewentualnych działań organów nadzorczych w związku z przetwarzaniem Danych Osobowych Klienta w ramach niniejszej umowy i na polecenie Powierzającego.

(2) W przypadku wysunięcia przez Wykonawcę wobec Powierzającego żądania podjęcia działań określonych w ustępie 1 Wykonawca pozostawi Powierzającemu w stosunku wewnętrznym wyłączną kontrolę nad obroną przed Roszczeniami Osób Trzecich i będzie w miarę możliwości wspierać Powierzającego przy odpieraniu tych roszczeń na koszt Powierzającego.

(3) Powierzający nie ma obowiązku zwolnienia Wykonawcy z roszczeń określonych w ustępie 1, jeżeli Roszczenia Osób Trzecich wynikają (i) z naruszenia niniejszej umowy przez Wykonawcę lub (ii) w szczególności z anonimizacji Danych Osobowych Klienta i wykorzystywania tych zanonimizowanych danych dla własnych celów Wykonawcy.

12. Załączniki

Załącznik nr 1: EquipCare – Środki techniczne i organizacyjne

Załącznik nr 2: Szczególne zalecenia Powierzającego w sprawie przekazywania Danych Osobowych Klienta podmiotom trzecim

Załącznik nr 1

EquipCare – Środki techniczne i organizacyjne

Poniżej opisane zostały środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie danych osobowych w EquipCare zgodnie z art. 32 RODO. O ile nie ustalono inaczej, środki te obowiązują zarówno Wykonawcę Wacker Neuson jak i podwykonawcę Trackunit. Środki dotyczące tylko jednego podmiotu przetwarzającego zostały wyraźnie określone.

Kontrola dostępu

Dostęp do wszystkich pomieszczeń, w których przetwarzane są dane osobowe, jest zabezpieczony.
Środki bezpieczeństwa są następujące:

a) Wszystkie ważne urządzenia wyposażone są w kontrolę dostępu.
b) Pracownicy otrzymują klucze/karty dostępu.
c) Każda osoba odpowiada za bezpieczeństwo własnego klucza/karty, a fakt utraty lub sytuacje, w których zagrożone może być bezpieczeństwo budynku, zgłosi w ciągu 24 godzin.
d) Zabronione jest wypożyczanie, duplikowanie, zmiana lub korzystanie z kluczy/kart w celu udostępnienia pomieszczeń osobom nieupoważnionym.
e) Istnieją czynne systemy alarmowe.
f) Goście muszą być rejestrowani i protokołowani.
g) Utworzony został program Due Diligence dla wszystkich klientów i dostawców, w tym dla osób mających dostęp do pomieszczeń, takich jak służby sprzątające i ochroniarskie.
h) Kontrole dostępu do części chronionych minimalizują zagrożenie uszkodzeniem lub awarią systemów.
i) Dostęp do pomieszczeń serwerowni/pomieszczeń komunikacyjnych ograniczony jest do kręgu osób upoważnionych.
j) Fizyczne nośniki danych przechowywane są w zamykanych szafach.

Dostęp do systemu

Dostęp do systemów przetwarzania danych mają wyłącznie osoby upoważnione i autoryzowane.
Środki bezpieczeństwa są następujące:

a) Użytkownicy autoryzowani są każdorazowo jednoznaczną nazwą użytkownika i hasłem.
b) Dostęp zabezpieczony jest przy pomocy sieci VPN i ew. MFA (uwierzytelniania wielopoziomowego).
c) Zdalny dostęp osób trzecich do systemów nie jest w żadnym momencie możliwy, chyba że za wyraźnym zezwoleniem. W razie udzielenia takiego dostępu jest on przez cały czas monitorowany.
d) Udostępnione usługi zabezpieczone są przed nieautoryzowanym dostępem z zewnątrz firewallami i szyframi.
e) Usługi wykonywane przez Trackunit monitorowane są całodobowo przy pomocy narzędzi do stałego skanowania nieprawidłowości, tak aby zapewnić najwyższy stopień bezpieczeństwa.
f) Na serwerach i stanowiskach komputerowych w sposób ciągły przeprowadzane są aktualizacje bezpieczeństwa, chroniące przed złośliwym wykorzystywaniem słabych punktów w stosowanych aplikacjach.
g) Trackunit przeniósł dane osobowe (pełne imię i nazwisko, nazwa użytkownika, hasło, e-mail itp.) na nowego zarządcę tożsamości (Identity Management Provider). Powyższa migracja zapewnia przechowywanie danych osobowych w postaci całkowicie zaszyfrowanej u nowoczesnego zarządcy tożsamością (okta.com), posiadającego certyfikaty SOC2 Typ1 i 2, ISO 27001, ISO27018 i CSA Star Level 2.

h) Osoby mające dostęp do chronionych części systemów informatycznych otrzymują od administratorów IT specjalne hasło. Hasło to powinno być regularnie zmieniane i spełniać zdefiniowane wymogi dotyczące długości i złożoności.
i) Komputery i inne urządzenia powinny być używane zgodnie z regulaminami wewnętrznymi, np. po opuszczeniu pomieszczenia muszą być blokowane (Clear Screen Policy).
j) W firmie Trackunit wszyscy programiści odbywają obowiązkowe szkolenia w zakresie bezpieczeństwa.

Dostęp do danych

Osoby upoważnione do korzystania z systemów przetwarzania danych otrzymują dostęp jedynie do takich danych osobowych, do których są uprawnione.
Środki bezpieczeństwa są następujące:
a) Pracownicy upoważnieni do przetwarzania danych osobowych zostali zobowiązani do zachowania poufności i podlegają stosownemu ustawowemu obowiązkowi zachowania tajemnicy.
b) Dostęp pracowników do systemów produkcyjnych, środowisk programistycznych i usług ograniczony jest do tych, które są konieczne do celów służbowych.
c) Dostęp zostaje bezwzględnie zmieniony lub usunięty, jeżeli dana osoba zmieni stanowisko pracy bądź pracodawcę.
d) Wewnętrzny dział IT przeprowadza regularne kontrole w celu zapewnienia zgodności wszystkich udzielonych praw ze stanowiskiem służbowym poszczególnych pracowników.
e) Nikt, kto nie został przeszkolony lub w inny sposób stosownie poinformowany o jego obowiązkach w zakresie bezpieczeństwa, nie ma dostępu do zasobów informatycznych.

Przekazywanie danych

Dane osobowe podczas przekazywania chronione są przed ich odczytem, skopiowaniem lub usunięciem przez osoby nieupoważnione.
Środki bezpieczeństwa są następujące:
a) Urządzenie RAW w firmie Trackunit używa szyfru blokowania Advanced Encryption Standard (AES).
b) Zaszyfrowane oprogramowanie firmowe przesyłane jest przez Trackunit IRIS do urządzeń wraz z bezpiecznym hashem dla celów kontroli autentyczności i integralności.
c) Komunikacja pomiędzy usługami (Manager, Go, On) a IRIS zaimplementowana jest jako interfejs REST oparty o protokół HTTPS.
d) Oficjalny interfejs Trackunit-API używa protokołu HTTPS.
e) Komunikacja pomiędzy Trackunit RAW a IRIS oparta jest na sieci GSM i chroniona jest kodem GSM. Do celów transmisji danych stosowany jest zastrzeżony protokół na IP/UDP. SMS-y używane są okazjonalnie do zarządzania urządzeniami.
f) Komunikacja przychodząca na urządzenia RAW poddawana jest każdorazowo walidacji przy pomocy różnych środków w celu zapewnienia akceptacji przez te urządzenia wyłącznie autoryzowanych zapytań.
g) Poza kodem GSM Trackunit wprowadzi szyfrowanie end-to-end dla komunikacji m2m pomiędzy urządzeniem a chmurą.

Integralność i dostępność

Poniższe działania zapewniają zachowanie kompletności i prawidłowości danych osobowych podczas ich przetwarzania. Gwarantują one ochronę danych osobowych przed niezamierzonym zniszczeniem lub utratą oraz możliwość odzyskania lub dostępności danych osobowych w razie jakiegoś incydentu.
Środki bezpieczeństwa są następujące:
a) Bazy danych są codziennie zabezpieczane, aby umożliwić przywrócenie działania systemu w razie awarii.

b) Trackunit stosuje proces zarządzania zdarzeniami Incident Management Process z całodobowym monitoringiem krytycznych usług.
c) Trackunit opracował plan obsługi incydentów związanych z bezpieczeństwem Incident Response Plan, który w przypadku naruszenia musi być bezwzględnie przestrzegany. Określa on podział kompetencji oraz harmonogram dla wszystkich uczestników w celu dotrzymania terminów zgłoszenia zgodnie z RODO. Powyższy plan obejmuje także komunikację zewnętrzną.
d) Terminy dotyczące usuwania i przechowywania określone są w obowiązujących przepisach prawa.

Porozumienia w sprawie powierzenia przetwarzania danych

Przetwarzane na zlecenie klienta dane osobowe podlegają przetwarzaniu wyłącznie na podstawie stosownego porozumienia i zgodnie ze stosownymi poleceniami klienta. Ze wszystkimi spółkami, które mogą mieć dostęp do danych osobowych, zawarte zostały porozumienia w sprawie powierzenia przetwarzania danych zgodnie z artykułem 28 RODO.

Rozdzielanie danych

Dane osobowe, gromadzone do odrębnych celów, przetwarzane są odrębnie.
Środki bezpieczeństwa są następujące:
a) Dane osobowe pobrane przez urządzenia/maszyny automatycznie przyporządkowywane są różnym klientom. Dane pozostają zawsze w oddzieleniu od klientów.
b) Klient ma dostęp wyłącznie do własnych danych osobowych.
c) Dane klientów traktowane są zawsze w sposób poufny. Prawa audytorskie, ewentualnie udzielane klientom, wyłączają w każdym przypadku prawo wzgl. możliwość wglądu do danych innych klientów.

Compliance

Wdrożone zostały procesy regularnej kontroli, oceny i oceny skuteczności środków technicznych i organizacyjnych służących zapewnieniu bezpieczeństwa przetwarzania.
a) Wacker Neuson SE wyznaczył inspektora ochrony danych (IOD). Pytania do niego i sprawy związane z przetwarzaniem danych należy kierować pod adres datenschutz@wackerneuson.com. Trackunit również wyznaczył inspektora ochrony danych.
b) Wdrożone zasady i wytyczne dotyczące ochrony danych podlegają corocznej kontroli i ew. aktualizacji.
c) Wprowadzona została procedura oceny skutków dla ochrony danych w celu dokonywania oceny skutków przetwarzania dla ochrony danych osobowych zgodnie z art. 35 RODO.
d) Podjęte zostaną odpowiednie kroki, aby zapewnić znajomość i stosowanie przez personel środków technicznych i organizacyjnych opisanych w niniejszym dokumencie. Wszyscy pracownicy muszą odbywać w odpowiednich odstępach czasowych szkolenia prowadzone przez IOD.
e) Trackunit co dwa tygodnie realizuje dla wszystkich klientów i dostawców program Due Diligence w celu identyfikacji ryzyk.

Załącznik nr 2

Szczególne zalecenia Powierzającego w sprawie przekazywania Danych Osobowych Klienta podmiotom trzecim

Po zawarciu Porozumienia W Sprawie Świadczenia aplikacja telematyczna umożliwia Wykonawcy, innym przedsiębiorstwom Grupy Wacker Neuson oraz dystrybutorom Wykonawcy dostęp do Danych Osobowych Klienta dla realizacji własnych celów biznesowych (np. wykonywania usług w ramach Serwisów EquipCare na wniosek Powierzającego lub prac rozwojowych nad produktem).

Niżej wymienionym odbiorcom udostępnione zostaną Dane Osobowe Klienta do ich niżej wymienionych własnych celów biznesowych:

Odbiorca	Własny cel biznesowy
Wacker Neuson SE	• druga linia wsparcia (na konkretny wniosek Powierzającego o wsparcie)
Spółka produkcyjna (Grupy Wacker Neuson), która wyprodukowała maszynę, z której przekazane zostały Dane Osobowe Klienta.	• druga linia wsparcia (na konkretny wniosek Powierzającego o wsparcie) • prace rozwojowe nad produktem • rozpatrywanie ewentualnych roszczeń z tytułu rękojmi i gwarancji
Spółka dystrybucyjna (Grupy Wacker Neuson), która sprzedała maszynę, z której przekazane zostały Dane Osobowe Klienta, bezpośrednio na rzecz Powierzającego, ewentualnego poprzedniego posiadacza lub w inny sposób w charakterze pośrednika.	• pierwsza linia wsparcia (na konkretny wniosek Powierzającego o wsparcie) • rozpatrywanie ewentualnych roszczeń z tytułu rękojmi i gwarancji
Dystrybutor (Partner Dystrybucyjny), który sprzedał maszynę, z której przekazane zostały Dane Osobowe Klienta, na rzecz Powierzającego lub ewentualnego poprzedniego posiadacza.	• pierwsza linia wsparcia (na konkretny wniosek Powierzającego o wsparcie) • rozpatrywanie ewentualnych roszczeń z tytułu rękojmi i gwarancji

Powierzający niniejszym wydaje Wykonawcy polecenie przekazania Danych Osobowych Klienta w drodze udzielenia prawa dostępu wyżej wymienionym odbiorcom do wyżej wymienionych celów, o ile jest to konieczne dla wyżej określonych własnych celów biznesowych tych odbiorców. W tym zakresie odbiorcy ci działają każdorazowo w charakterze administratora w rozumieniu art. 4 ust. 7 RODO.

Jeżeli Wykonawca sam jest odbiorcą Danych Osobowych Klienta, Wykonawca niniejszym zobowiązuje się wobec Powierzającego do przetwarzania Danych Osobowych Klienta wyłącznie w wyżej określonych celach i unikania w każdy możliwy sposób bezpośredniej identyfikacji osób, których dane dotyczą. Wykonawca zobowiązuje się także nie sporządzać kopii Danych Osobowych Klienta, lecz przetwarzać Dane Osobowe Klienta wyłącznie na prowadzonym przez Wykonawcę portalu (zgodnie z definicją zawartą w Porozumieniu W Sprawie Świadczenia). Powyższe nie ogranicza możliwości sporządzania kopii informacji zanonimizowanych.