Umowa z podmiotem przetwarzającym (zgodnie z art. 28 GDPR)

pomiędzy

Użytkownikiem (według definicji zawartej w Umowie Głównej)

(dalej zwanym „**Zleceniodawcą**")

a

TB Digital Services GmbH, Oskar-Schlemmer-Str. 19 - 21, 80807 Monachium

(dalej zwanym „**Zleceniobiorcą**")
(Zleceniodawca i Zleceniobiorca są dalej zwani indywidualnie „**Stroną**", a łącznie „**Stronami**").

Wstęp

(A) Niniejsza umowa z podmiotem przetwarzającym (dalej zwana „**Umową**") ma zastosowanie do wszystkich działań, przy których Zleceniobiorca ma styczność z danymi osobowymi (według definicji zawartej poniżej w punkcie 1.5) Zleceniodawcy, dostawcy zewnętrznego lub innych osób w związku z działalnością opisaną w punkcie 2 według Ogólnych Warunków Ramowych dotyczących użytkowania platformy i ew. zawartych na ich podstawie indywidualnych umów o świadczenie usług dodatkowych (dalej: „**Umowa Główna**").

(B) Na warunkach niniejszej Umowy Zleceniodawca występuje jako podmiot odpowiedzialny, a Zleceniobiorca jako podmiot przetwarzający zlecenie w ramach przetwarzania danych dotyczących zlecenia według art. 28 GDPR (ogólnego rozporządzenia o ochronie danych) (według poniższej definicji).

Strony uzgadniają zatem, co następuje:

1 Definicje i interpretacja

1.1 „**Prawo Europejskie**" oznacza obowiązujące prawo Unii Europejskiej, obowiązujące prawo obecnych państw członkowskich Unii Europejskiej oraz obowiązujące prawo każdego państwa, które stanie się później państwem członkowskim Unii Europejskiej.

1.2 „**Europejskie Prawo Ochrony Danych**" oznacza obowiązujące prawo Unii Europejskiej dotyczące przetwarzania danych osobowych (w szczególności rozporządzenie GDPR), obowiązujące prawo obecnych państw członkowskich Unii Europejskiej dotyczące przetwarzania danych osobowych (w szczególności ustawa BDSG w każdorazowo obowiązującej wersji) oraz obowiązujące prawo każdego państwa, które stanie się później państwem członkowskim Unii Europejskiej, dotyczące przetwarzania danych osobowych.

1.3 „**Rozporządzenie**" oznacza „ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)."

1.4 „**Ustawa**" oznacza niemiecką ustawę o ochronie danych.

1.5 „**Dane Osobowe**" mają znaczenie zdefiniowane w Ustawie/Rozporządzeniu.

2 Przedmiot przetwarzania danych / Obowiązki Zleceniodawcy

2.1 Niniejsza Umowa reguluje zobowiązania Stron w związku z przetwarzaniem danych osobowych Zleceniodawcy przez Zleceniobiorcę w ramach Umowy Głównej wskazanej w Załączniku 1.

2.2 Przedmiot i czas przetwarzania, rodzaj i cel przetwarzania, rodzaj danych osobowych, kategorie osób oraz obowiązki i prawa podmiotu odpowiedzialnego wynikają z Załącznika 1 do niniejszej Umowy i opisu zakresu usług z Umowy Głównej.

2.3 Zleceniodawca pozostaje podmiotem odpowiedzialnym w rozumieniu GDPR i gwarantuje dopuszczalność przetwarzania danych osobowych odnoszących się do osób, których to dotyczy (kierowców i ew. innych osób). W związku z tym Zleceniodawca realizuje w szczególności swój kompleksowy obowiązek udzielenia informacji i gwarantuje, że istniej podstawa prawna w zakresie prawa ochrony danych dotycząca przetwarzania danych osobowych (np. zawarcie porozumienia zakładowego, ograniczenie przetwarzania do celów stosunku zatrudnienia).

3 Obowiązki Zleceniobiorcy

3.1 Zleceniobiorca przetwarza dane osobowe Zleceniodawcy wyłącznie w celach wskazanych w Załączniku 1 oraz w ramach Umowy Głównej oraz na zlecenie i zgodnie ze wskazówkami Zleceniodawcy udokumentowanymi w Załączniku 1; Zleceniobiorca nie przetwarza danych osobowych na warunkach niniejszej Umowy w żadnych innych celach. Nie ma to wpływu na przetwarzanie poza zakresem niniejszej Umowy do celów własnych według punktu 8.3.4 Umowy Głównej. Kopie lub duplikaty danych osobowych nie mogą być sporządzane bez wiedzy Zleceniodawcy. Wyjątkiem są kopie bezpieczeństwa, które są wymagane dla zagwarantowania prawidłowego przetwarzania danych, oraz dane, które są niezbędne z uwagi na przestrzeganie ustawowych obowiązków przechowywania.

3.2 Po zakończeniu świadczenia usług w zakresie przetwarzania Zleceniobiorca jest zobowiązany do przekazania Zleceniodawcy wszystkich danych osobowych Zleceniodawcy i/lub usunięcia ich po swojej stronie z zachowaniem wymogów przepisów o ochronie danych, według wyboru Zleceniodawcy, o ile nie jest to sprzeczne z wymogami dotyczącymi ustawowych terminów przechowywania danych oraz o ile Zleceniobiorca nie przetwarza ich do celów własnych poza zakresem niniejszej Umowy według

punktu 8.3.4 Umowy Głównej. Postanowienie to dotyczy również materiałów testowych i materiałów do utylizacji. Zleceniobiorca jest zobowiązany do potwierdzenia Zleceniodawcy na piśmie całkowitego usunięcia lub wydania danych Zleceniobiorcy na jego żądanie, ze wskazaniem daty.

3.3 Jeżeli zakres zlecenia to obejmuje, Zleceniobiorca wspiera Zleceniodawcę przy realizacji praw osób, których to dotyczy (informacja, sprostowanie, sprzeciw, usunięcie) po odpowiednim poleceniu Zleceniodawcy.

3.4 Zleceniobiorca potwierdza, że – o ile jest to wymagane przepisami prawa – wyznaczył w firmie osobę odpowiedzialną za ochronę danych (por. § 38 ustawy BDSG, art. 37 GDPR).

3.5 Zleceniobiorca zobowiązuje się do niezwłocznego poinformowania Zleceniodawcy o rezultacie kontroli prowadzonych przez organy nadzoru ochrony danych, o ile kontrole te są związane z przetwarzaniem danych Zleceniodawcy. W razie stwierdzenia nieprawidłowości Zleceniobiorca jest zobowiązany do ich usunięcia w stosownym terminie i poinformowania Zleceniodawcy o tym fakcie.

3.6 Przetwarzanie danych przez Zleceniobiorcę i podwykonawców zaakceptowanych przez Zleceniodawcę odbywa się wyłącznie na terytorium Republiki Federalnej Niemiec, w państwie członkowskim Unii Europejskiej lub innym państwie będącym sygnatariuszem Umowy o Europejskim Obszarze Gospodarczym. Każde przeniesienie do innego kraju (dalej zwanego „**krajem trzecim**") wymaga uprzedniego uzyskania wyraźnej zgody Zleceniodawcy i może nastąpić wyłącznie po spełnieniu szczególnych warunków eksportu danych do krajów trzecich (por. art. 40 i nast. GDPR). W tym zakresie niezbędne są informacje określone w Załączniku 1, a w razie potrzeby należy dołączyć dodatkowe dokumenty (umowy).

3.7 Zleceniobiorca jest zobowiązany do zapoznania osób zatrudnionych do wykonywania prac z obowiązującymi postanowieniami dotyczącymi ochrony danych oraz zobowiązania ich do zachowania poufności danych (por. art. 28 GDPR, ust. 3 b)) oraz do zagwarantowania poprzez odpowiednie działania, aby pracownicy ci przetwarzali dane osobowe wyłącznie zgodnie ze wskazówkami Zleceniodawcy.

3.8 Zleceniobiorca nadzoruje przestrzeganie przepisów dotyczących ochrony danych, wynikających z niniejszej Umowy i udokumentowanych wytycznych Zleceniodawcy, regularnie w trakcie całego okresu obowiązywania Umowy. Zleceniobiorca jest zobowiązany do przedstawienia na żądanie Zleceniodawcy rezultatów kontroli, o ile są one istotne dla przetwarzania danych Zleceniodawcy. Środki nadzoru są opisane w koncepcji ochrony danych, którą należy przedstawić Zleceniodawcy na żądanie.

3.9 Z uwagi na rodzaj przetwarzania i w miarę możliwości przy zastosowaniu odpowiednich środków technicznych i organizacyjnych Zleceniobiorca jest zobowiązany do zapewnienia Zleceniodawcy wsparcia w zakresie spełnienia jego obowiązku dotyczącego udzielania odpowiedzi na wnioski w odniesieniu do praw osób wskazanych w Rozdziale III Rozporządzenia. Zleceniodawca jest zobowiązany do pokrycia kosztów powstałych po stronie Zleceniobiorcy w tym zakresie.

3.10 Z uwagi na rodzaj przetwarzania i dostępnych dla niego informacji Zleceniobiorca jest zobowiązany do wspierania Zleceniodawcy w zakresie spełnienia obowiązków wskazanych w Art. 32–36 Rozporządzenia.

4 Techniczne i organizacyjne środki ochrony danych

4.1 Zleceniobiorca podejmie odpowiednie działania techniczne i organizacyjne w zakresie ochrony danych (por. art. 32 GDPR). Zleceniobiorca jest w szczególności zobowiązany do realizowania środków technicznych i organizacyjnych uzgodnionych w Załączniku 2 do niniejszej Umowy. Środki te będą dostosowywane przez Zleceniobiorcę w trakcie trwania zlecenia w miarę zmian technicznych i organizacyjnych, bez zmniejszenia poziomu ochrony. Istotne zmiany wymagają uzgodnienia na piśmie.

4.2 Zleceniobiorca jest zobowiązany do udowodnienia na żądanie Zleceniodawcy faktycznego stosowania środków technicznych i organizacyjnych.

4.3 Zleceniobiorca jest zobowiązany do prowadzenia odpowiedniej dokumentacji przetwarzania danych, na podstawie której Zleceniodawca może udowodnić prawidłowe przetwarzanie danych. Dowód może nastąpić również w drodze zatwierdzonego postępowania certyfikacyjnego zgodnie z Art. 42 Rozporządzenia.

5 Podwykonawcy

5.1 Zleceniobiorca otrzymuje niniejszym zgodę na zaangażowanie podwykonawców wskazanych w Załączniku 1.

5.2 Niniejszym zezwala się generalnie na zaangażowanie dalszych podwykonawców. Zleceniobiorca będzie jednak informować Zleceniodawcę o każdej zamierzonej zmianie w zakresie zaangażowania dodatkowego podwykonawcy lub zastąpienia podwykonawcy; Zleceniodawca może zgłosić sprzeciw wobec zamierzonych zmian. Za relację podwykonawstwa w rozumieniu niniejszej regulacji nie uważa się takich usług, z których Zleceniobiorca korzysta u osób trzecich w ramach świadczenia dodatkowego dla wsparcia przy realizacji zlecenia. Do tego zakresu zalicza się np. usługi telekomunikacyjne, usługi porządkowe, audytorskie lub utylizację nośników danych. W celu zagwarantowania ochrony i bezpieczeństwa danych Zleceniodawcy Zleceniobiorca jest jednak zobowiązany, również w odniesieniu do usług dodatkowych zlecanych na zewnątrz, do zawierania odpowiednich i zgodnych z przepisami prawa uzgodnień kontraktowych oraz do stosowania środków kontroli.

5.3 Jeżeli Zleceniobiorca korzysta z usług podwykonawcy, Zleceniobiorca jest zobowiązany do zapewnienia, że na podwykonawcę nałożone zostaną takie same obowiązki ochrony danych, jakie są nałożone na Zleceniobiorcę na podstawie niniejszej Umowy, w drodze (i) umowy zawieranej pomiędzy podwykonawcą a Zleceniobiorcą lub (ii) innego instrumentu prawnego według Europejskiego Prawa Ochrony Danych. Zleceniobiorca powinien przy tym w szczególności zadbać o to, aby podwykonawca

zaoferował wystarczające gwarancje zastosowania odpowiednich środków technicznych i organizacyjnych w taki sposób, aby przetwarzanie danych osobowych odbywało się zgodnie z wymogami GDPR. Na pisemne żądanie Zleceniodawcy, Zleceniobiorca udzieli Zleceniodawcy informacji o istotnych postanowieniach umowy i realizacji zobowiązań podwykonawcy w zakresie ochrony danych osobowych, w razie potrzeby w drodze wglądu do odpowiednich dokumentów umowy. Zleceniobiorca może przy tym zaczernić warunki handlowe. Zleceniodawca jest zobowiązany do zachowania poufności pozyskanych informacji.

6 Prawo kontroli

6.1 Zleceniodawca ma prawo do kontrolowania bądź zlecenia kontroli przestrzegania zobowiązań wynikających z niniejszej Umowy (łącznie z udzielonymi wytycznymi) samodzielnie lub za pośrednictwem odpowiedniej osoby trzeciej wyznaczonej przez Zleceniodawcę.

6.2 Zleceniobiorca zapewni Zleceniodawcy odpowiednie wsparcie w zakresie kontroli. W szczególności Zleceniobiorca zapewni dostęp do obiektów przetwarzania danych oraz udzieli niezbędnych informacji.

6.3 Jeżeli kontrola wykaże, że Zleceniobiorca i/lub przetwarzanie nie spełnia wymogów niniejszej Umowy i/lub Europejskiego Prawa Ochrony Danych, Zleceniobiorca podejmie wszelkie środki korygujące, które są wymagane dla zagwarantowania spełnienia wymogów niniejszej Umowy i/lub Europejskiego Prawa Ochrony Danych.

6.4 Koszty powstałe po stronie Zleceniodawcy wskutek przeprowadzenia kontroli pokrywa sam Zleceniodawca. Zleceniobiorca może żądać od Zleceniodawcy pokrycia kosztów powstałych dla Zleceniobiorcy wskutek przeprowadzenia kontroli, jeżeli Zleceniodawca wykonuje lub zleca wykonanie kontroli częściej niż raz w roku kalendarzowym.

6.5 Kontrole u Zleceniobiorcy powinny być zapowiadane z odpowiednim wyprzedzeniem i nie mogą nadmiernie zakłócać prowadzenia działalności Zleceniobiorcy.

7 Obowiązek udzielenia informacji

Zleceniobiorca niezwłocznie powiadomi Zleceniodawcę, jeżeli którekolwiek z wytycznych udzielonych przez Zleceniodawcę będą zdaniem Zleceniodawcy niezgodne z Europejskim Prawem Ochrony Danych. Wytyczne, które zostały słusznie zakwestionowane, nie muszą być realizowane, dopóki nie zostaną zmienione lub wyraźnie potwierdzone przez Zleceniodawcę. Zleceniobiorca nie jest zobowiązany do materialno-prawnego sprawdzania wytycznych.

W razie stwierdzenia błędów lub nieprawidłowości przetwarzania danych lub przy podejrzeniu naruszenia ochrony danych (dalej zwanych łącznie „**Zdarzeniem**”), Zleceniobiorca jest zobowiązany do niezwłocznego przekazania Zleceniodawcy stosownych informacji. Zleceniodawca jest zobowiązany do

udokumentowania Zdarzenia łącznie z wszystkimi faktami, jego skutkami i wszystkimi środkami podjętymi w celu ich usunięcia, a na żądanie Zleceniodawcy do niezwłocznego przekazania mu tych udokumentowanych informacji w formie pisemnej lub elektronicznej.

8 Odpowiedzialność i zwolnienie z odpowiedzialności

8.1 Zleceniobiorca ponosi odpowiedzialność za szkody powstałe wskutek umyślnego postępowania i/lub rażącego zaniedbania Zleceniobiorcy bądź jego wykonawców. Zleceniobiorca odpowiada za szkody wynikające ze zwykłego zaniedbania Zleceniobiorcy bądź jego wykonawców wyłącznie w przypadku naruszenia głównego zobowiązania. Obowiązkami głównymi są istotne obowiązki umowne, które umożliwiają prawidłowe realizowanie Umowy oraz na których spełnieniu Zleceniodawca polega i może polegać. W przypadku zwykłego zaniedbania w zakresie naruszenia takich obowiązków głównych odpowiedzialność Zleceniobiorcy jest ograniczona do typowo przewidywalnych szkód.

8.2 Zleceniodawca zwolni Zleceniobiorcę z wszelkich roszczeń osób trzecich (łącznie z podmiotami danych i/lub organami ds. ochrony danych), szkód i nakładów wynikających z naruszenia przez Zleceniodawcę postanowień niniejszej Umowy i/lub Europejskiego Prawa Ochrony Danych; postanowienie to nie ma zastosowania, jeżeli Zleceniodawca nie ponosi winy za dane naruszenie lub jeżeli Zleceniobiorca przyczynił się do danego naruszenia.

9 Okres obowiązywania

Okres obowiązywania niniejszej Umowy odpowiada okresowi obowiązywania Umowy Głównej. Wraz z zakończeniem Umowy Głównej, niezależnie od przyczyn, następuje również automatyczne zakończenie niniejszej Umowy. Postanowienie to nie ma wpływu na możliwość rozwiązania umowy z ważnej przyczyny.

10 Pozostałe

10.1 Świadczenia Zleceniobiorcy według niniejszej Umowy są uważane za rozliczone według regulacji dotyczącej wynagrodzenia, zawartej w Umowie Głównej.

10.2 W przypadku zagrożenia danych osobowych Zleceniodawcy w siedzibie Zleceniobiorcy wskutek środków podjętych przez osoby trzecie (na przykład w drodze zastawu lub konfiskaty), przez postępowanie upadłościowe lub likwidacyjne bądź wskutek innych porównywalnych wydarzeń, Zleceniobiorca jest zobowiązany do niezwłocznego powiadomienia Zleceniodawcy o tym fakcie.

10.3 Ewentualna nieskuteczność któregokolwiek z postanowień niniejszej Umowy nie wpływa na skuteczność pozostałych postanowień. W przypadku nieskuteczności jednej klauzuli Strony uzgodnią regulację zastępczą, ukierunkowaną pod względem merytorycznym i ekonomicznym na cel Umowy.

10.4 Na wypadek wystąpienia Wielkiej Brytanii z Unii Europejskiej Zleceniobiorca zobowiązuje się już teraz do zawarcia wszelkich porozumień i do podjęcia wszelkich działań, które są niezbędne dla zapewnienia przedmiotowego przetwarzania danych w Wielkiej Brytanii w momencie wystąpienia zgodnie z przepisami prawa o ochronie danych. Jeżeli w momencie wystąpienia brak będzie pozytywnej decyzji Komisji Europejskiej w sprawie adekwatności, są to z dzisiejszego punktu widzenia w szczególności standardowe klauzule ochrony danych zgodnie z art. 46 ust. 2 c) dotyczące przekazywania danych osobowych do podmiotów przetwarzających zlecenie w krajach trzecich, w których nie ma zagwarantowanego odpowiedniego poziomu ochrony.

Jeżeli Zleceniobiorca nie spełni tych obowiązków, Zleceniodawca ma prawo do żądania od Zleceniobiorcy, ze skutkiem od momentu wystąpienia Wielkiej Brytanii z Unii Europejskiej, świadczenia właściwych usług przez przedsiębiorstwo powiązane lub przez część przedsiębiorstwa posiadającego stałą siedzibę na terenie Unii Europejskiej, bez dodatkowych nakładów lub dodatkowych kosztów dla Zleceniodawcy.

10.5 Niniejsza Umowa z podmiotem przetwarzającym ostała sporządzona w 18 wersjach językowych, przy czym w razie rozbieżności decydujące znaczenie ma niemiecka wersja oryginalna.

10.6 Niniejsza Umowa podlega przepisom prawa Republiki Federalnej Niemiec, z wyłączeniem CISG. Sądem właściwym miejscowo jest wyłącznie sąd w Monachium.

10.7 Następujące załączniki stanowią integralną część Umowy:

Załącznik 1 – Opis przetwarzania danych dotyczących zlecenia
Załącznik 2 – Środki techniczne i organizacyjne

ZAŁĄCZNIK 1 – Opis przetwarzania danych dotyczących zlecenia

1 Umowa Główna

Umową Główną w rozumieniu punktu 2.1 części głównej Umowy są „Ogólne Warunki Ramowe dotyczące użytkowania platformy".

Tytuł / Strony: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 Monachium/ **Użytkownik**

2 Przedmiot i okres realizacji zlecenia

Przedmiot zlecenia wynika z punktu 1 (*Przedmiot*) i punktu 8 (*Dane Użytkownika i ochrona danych*) Umowy Głównej; okres obowiązywania zlecenia wynika z punktu 7 (*Zawarcie umowy, okres obowiązywania umowy i prawo do wypowiedzenia*) Umowy Głównej.

3 Zakres, rodzaj i cel przetwarzania danych / środki w zakresie przetwarzania danych

Zakres, rodzaj i cel przetwarzania danych osobowych wynikają z punktu 8 Umowy Głównej.

Szczegółowy opis przedmiotu zlecenia w odniesieniu do zakresu, rodzaju i celu:

Aby móc świadczyć usługi oferowane przez Zleceniobiorcę (zgodnie z definicją zawartą w Umowie Głównej), Zleceniobiorca musi pozyskiwać dane osobowe Zleceniodawcy za pośrednictwem Pojazdów Połączonych lub Urządzeń Mobilnych (oraz w razie potrzeby dane osobowe przekazane od dostawcy zewnętrznego, z którym Użytkownik uzgodnił świadczenie usług zewnętrznych) w zakresie wymaganym dla świadczenia usług, oraz przekazywać je do platformy Zleceniobiorcy i w niej zapisywać. Zleceniobiorca będzie przetwarzać dane zapisane na platformie w zakresie niezbędnym do świadczenia usług (w tym w celu analizowania i oceny charakterystyki jazdy kierowców i użytkowania Pojazdu Połączonego lub Urządzenia Mobilnego na podstawie danych osobowych oraz przedstawiania Zleceniodawcy ofert specjalnie przystosowanych do jego potrzeb, takich jak szkolenia dla kierowców, elementy wyposażenia oraz propozycje zwiększenia efektywności). Dokładny zakres, rodzaj i cel są w szczególności określone w dodatkowo zawieranych umowach indywidualnych.

4 Krąg podmiotów danych (kategorie podmiotów danych)

Przetwarzanie danych dotyczących zlecenia dotyczy następujących kręgów osób:

- **Kierowcy i inni pracownicy** (pracownicy spółki własnej Zleceniodawcy), np. pracownicy, stażyści, kandydaci, byli pracownicy*;*
- **Kierowcy**, którzy nie są pracownikami;

- **Osoby do kontaktu** w zakresie przeładunku/rozładunku lub ze strony innych kontrahentów Zleceniodawcy; oraz
- **Pracownicy koncernu** (pracownicy innej grupy spółek Zleceniodawcy).

5 Rodzaj danych osobowych

Przetwarzanie danych dotyczących zlecenia obejmuje następujące rodzaje danych osobowych:

- Nazwisko kierowcy i numer identyfikacyjny kierowcy;
- Numer identyfikacyjny pojazdu;
- Dane lokalizacyjne;
- Dane dotyczące czasu kierowania pojazdem i odpoczynku;
- Dane dotyczące charakterystyki jazdy;
- Dane dotyczące stanu Pojazdu Połączonego;
- Dane dotyczące stanu przyczepy;
- Dane dotyczące stanu nadwozia lub naczepy, agregatów i innych elementów konstrukcyjnych pojazdów;
- Dane dotyczące stanu ew. połączonych urządzeń IOT;
- Dane dotyczące stanu Urządzeń Mobilnych;
- Dane dotyczące załadunku;
- Dane dotyczące zlecenia; oraz
- Dane kontaktowe osób do kontaktu w zakresie przeładunku/rozładunku lub ze strony innych kontrahentów Zleceniodawcy.

6 Udokumentowane wytyczne

Zleceniodawca niniejszym zleca Zleceniobiorcy przetwarzanie danych osobowych zgodnie z punktem 8 Umowy Głównej. Obejmuje to w szczególności przetwarzanie w następującym zakresie:

- Dane osobowe są przesyłane poprzez Pojazd Połączony lub Urządzenie Mobilne do platformy Zleceniodawcy w chmurze i tam są zapisywane.
- Dane osobowe są przetwarzane na podstawie niniejszej Umowy wyłącznie wówczas, gdy jest to wymagane dla spełnienia wymogów Umowy Głównej; postanowienie to nie ma wpływu na punkt 8.3.4 Umowy Głównej.
- Zleceniobiorca przekazuje dane osobowe do dostawcy zewnętrznego (zgodnie z definicją zawartą w Umowie Głównej), jeżeli oraz o ile takie przekazanie danych do dostawcy zewnętrznego jest wymagane, aby taki dostawca zewnętrzny mógł świadczyć swoje usługi (zgodnie z definicją zawartą w Umowie Głównej) na rzecz Zleceniodawcy.
- Zleceniobiorca będzie analizować i oceniać charakterystykę jazdy kierowców i użytkowania Pojazdów Połączonych na podstawie danych osobowych oraz bazując na tym przedstawiać Zleceniodawcy oferty

specjalnie przystosowane do jego potrzeb, takie jak szkolenia dla kierowców, elementy wyposażenia oraz propozycje zwiększenia efektywności.

7 Miejsce przetwarzania danych

- Niemcy.
- Zjednoczone Królestwo; o ile dane są przetwarzane dla celów hostingu IT i/lub wsparcia IT w obrębie Unii Europejskiej, zawarte zostały odpowiednie umowy o przetwarzanie danych dotyczących zlecenia.
- Jeżeli Zleceniobiorca korzysta z usług podwykonawców dla celów hostingu IT i/lub wsparcia IT poza terenem Unii Europejskiej (zob. punkt 8 niniejszego Załącznika 1), przekazywanie danych osobowych odbywa się na podstawie zawartych pomiędzy Zleceniobiorcą a podwykonawcą standardowych klauzul umownych/standardowych klauzul w zakresie ochrony danych dotyczących przekazywania danych osobowych podmiotom przetwarzającym w krajach trzecich zgodnie z art. 46 ust. 2 c) GDPR.

8 Podwykonawcy

Zleceniobiorca angażuje następujących podwykonawców (którzy w razie potrzeby mogą angażować dalszych podwykonawców):

Nr	Podwykonawca (firma, adres, osoba do kontaktu)	Przetwarzane kategorie danych	Etapy przetwarzania / cel przetwarzania danych przez podwykonawcę
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Wszystkie dane osobowe platformy, które są związane z częścią sprzedażową (tj. w zakresie których klient może zarejestrować się na platformie i składać zamówienia)	Hosting platformy
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Wszystkie dane osobowe platformy, które są związane z częścią sprzedażową (tj. w zakresie których klient może zarejestrować się na platformie i składać zamówienia)	Wsparcie IT dla platformy
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 USA https://aws.amazon.com/de/compliance/contact/	Wszystkie pozostałe dane osobowe Użytkowników, które są przekazywane Zleceniobiorcy za pośrednictwem pojazdu	Hosting platformy / wsparcie IT lub hosting platformy
4	Ew. w przyszłości zamiast numeru 3: Amazon Webservices (UE) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 USA https://aws.amazon.com/de/compliance/contact/	Wszystkie pozostałe dane osobowe Użytkowników, które są przekazywane Zleceniobiorcy za pośrednictwem pojazdu	Hosting platformy
5	MAN Service und Support GmbH Dachauer Straße 667	Wszystkie dane osobowe, które są wymagane do obsługi zapytań klientów w ramach wsparcia	Wsparcie poziomu 1

	80995 München Niemcy	poziomu 1 i 2	
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 USA	Wszystkie dane osobowe, które są wymagane do obsługi rozliczeń/realizacji zleceń	Hosting platformy (EU Tenant – hosting prowadzony przez Amazon Web Services (UE) – zob. punkt 4)
7	MAN Truck & Bus AG Dachauer Str. 667 80995 München Niemcy	Wszystkie pozostałe dane osobowe Użytkowników, które są przekazywane Zleceniobiorcy za pośrednictwem Pojazdu Połączonego i/lub Urządzenia Mobilnego	Hosting platformy
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Niemcy	Wszystkie pozostałe dane osobowe Użytkowników, które są przekazywane Zleceniobiorcy za pośrednictwem pojazdów TBM1/2	Hosting platformy
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Szwecja	Wszystkie pozostałe dane osobowe Użytkowników, które są przekazywane Zleceniobiorcy za pośrednictwem pojazdu	Hosting platformy
10	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hannover Niemcy	Wszystkie pozostałe dane osobowe Użytkowników, które są przekazywane Zleceniobiorcy za pośrednictwem pojazdu	Hosting platformy

ZAŁĄCZNIK 2 – Środki techniczne i organizacyjne

Środki techniczne i organizacyjne, które zostaną podjęte przez Zleceniobiorcę w celu zagwarantowania poziomu ochrony odpowiedniego dla ryzyka, są opisane w koncepcji ochrony danych dla platformy RIO i obejmują w szczególności następujące elementy:

1. Pseudonimizacja

Jeżeli dane osobowe są wykorzystywane do celów analizy, które mogą być wykonywane również z wykorzystaniem danych pseudonimizowanych, stosowane są techniki pseudonimizacji. Dla każdego pola danych definiuje się z góry, czy pole to musi zostać poddane pseudonimizacji, ponieważ umożliwiłoby to zidentyfikowanie osoby. Klucze pseudonimizacji są deponowane w „sejfie danych", dla którego ustanawiane jest maksymalne możliwe ograniczenie dostępu.

2. Szyfrowanie

Mobilne urządzenia końcowe komunikują się w sposób szyfrowany z punktem końcowym na podstawie indywidualnego certyfikatu urządzenia. Dane są transportowane w obrębie platformy RIO w formie zaszyfrowanej („Ubiquitous encryption" lub „encryption everywhere").

3. Gwarancja poufności

Wszyscy pracownicy są informowani o obowiązku zachowania tajemnicy i zobowiązani na piśmie do zachowania tajemnicy danych.

Wykorzystywana infrastruktura IT jest udostępniona przez Amazon Web Services (zwany dalej AWS) w ramach chmury (IaaS & PaaS). Kontrolę dostępu zapewnia operator centrum danych AWS: centra danych AWS o wysokim poziomie bezpieczeństwa wykorzystują nowoczesne elektroniczne środki nadzoru i systemy wielostopniowej kontroli dostępu. Centra danych są obsługiwane całodobowo przez wykwalifikowany personel ds. zabezpieczeń, a dostęp jest udzielany ściśle według zasady minimalnych uprawnień oraz wyłącznie w celu administrowania systemem.

Dostęp do komponentów sprzętowych (klientów) w TB Digital Services GmbH jest realizowany zgodnie z obowiązującymi, odpowiednimi dla każdego przypadku standardowymi środkami. Są to np. ograniczenia dostępu w formie instalacji oddzielających (krzyżaki obrotowe), instalacje nadzoru wideo, instalacja alarmowa i/lub system nadzoru, drzwi zabezpieczone elektronicznie lub mechanicznie, budynek z zabezpieczeniami antywłamaniowymi, udokumentowane uprawnienia dostępu (osoby odwiedzające, służby zewnętrzne) bądź zadeklarowane strefy bezpieczeństwa.

Środki kontroli dostępu obejmują środki zabezpieczenia urządzeń, zabezpieczenia sieci i zabezpieczenia aplikacji.

Jako zabezpieczenia urządzeń w pojeździe stosowane są różne środki: Mobilne urządzenia końcowe są wbudowane na stałe w pojeździe i są wyposażone w Secure Boot, tj. nie ma możliwości załadowania i uruchomienia obcego systemu operacyjnego. Mobilne urządzenia końcowe komunikują się w sposób szyfrowany z punktem końcowym na podstawie indywidualnego certyfikatu urządzenia. Dane są transportowane w obrębie platformy RIO w formie zaszyfrowanej („Ubiquitous encryption" lub „encryption everywhere"). Stan zabezpieczeń urządzeń końcowych jest aktualny poprzez regularne wgrywanie aktualizacji zabezpieczeń (zarządzanie poprawkami).

Jako zabezpieczenia sieci stosowane są także różne środki standardowe: Wdrożone są stosowne (odpowiednie do stanu techniki) wytyczne dotyczące haseł (długość hasła, stopień złożoności, okres ważności itp.). Powtórne wprowadzenie błędnej kombinacji identyfikatora użytkownika / hasła prowadzi do (czasowego) zablokowania identyfikatora użytkownika. Sieć firmowa jest zabezpieczona zaporą ogniową przed otwartymi sieciami bez zabezpieczeń. Wdrożony jest proces zapewniający regularne dostarczanie aktualizacji zabezpieczeń dla urządzeń mobilnych (proces OTA). W celu wykrywania lub unikania ataków na sieć firmową (Intranet) stosowane są odpowiednie technologie (np. systemy Intrusion Detection). Pracownicy są regularnie uczulani na kwestie zagrożeń i ryzyka.

Jako zabezpieczenia aplikacji stosowane są pewne środki standardowe:

Odpowiednie aplikacje są zabezpieczone przed dostępem osób niepowołanych poprzez stosowne mechanizmy uwierzytelniania i autoryzacji. Wdrożone są stosowne (odpowiednie do stanu techniki) wytyczne dotyczące haseł (długość hasła, stopień złożoności, okres ważności itp.). Dla aplikacji o szczególnym zapotrzebowaniu na ochronę stosowane są silne mechanizmy uwierzytelniające (np. token, PKI). Powtórne wprowadzenie błędnej kombinacji identyfikatora użytkownika / hasła prowadzi do (czasowego) zablokowania identyfikatora użytkownika. Dane wykorzystywane w danym procesie znajdują się w formie zaszyfrowanej na nośniku danych użytkowanym w formie mobilnej. Zrealizowane dostępy i próby dostępu do aplikacji są protokołowane. Wygenerowane pliki protokołu są przechowywane przez odpowiedni okres (minimum 90 dni) i (wyrywkowo) sprawdzane.

Uprawnienia użytkownika (w zakresie dostępu) są realizowane przy użyciu różnych środków, przy czym są one zasadniczo przypisane do identyfikowalnej osoby. Przydzielanie uprawnień odbywa się na odpowiedzialność osoby odpowiedzialnej za platformę i jest regularnie weryfikowane. Uprawnienia dostępu są przydzielane wyłącznie na podstawie zdefiniowanego i udokumentowanego procesu. Zmiany uprawnień dostępu są dokonywane zgodnie z zasadą czterech oczu i są dokumentowane w wersjonowanym pliku rejestru.

Jako zabezpieczenia kontroli dostępu lub sterowania dostępem stosowane są różne środki: Prawa dostępu są definiowane i dokumentowane w ramach koncepcji ról/uprawnień oraz są przydzielane odpowiednio do uwarunkowanych zadaniowo wymogów poszczególnych ról. Ustalone są określone role/uprawnienia dla administratorów technicznych (które – w miarę możliwości technicznych – nie umożliwiają dostępu do danych osobowych). Ustalone są określone role/uprawnienia dla wsparcia specjalistycznego (które nie obejmują technicznych praw administracyjnych).

Role/uprawnienia są definiowane i przydzielane – o ile jest to możliwe pod względem technicznym i organizacyjnym – przez różne osoby i w ramach weryfikowalnego procesu (akceptacji), z zachowaniem ograniczeń czasowych. Bezpośredni dostęp do bazy danych z obejściem koncepcji ról/uprawnień jest możliwy wyłącznie dla uprawnionych administratorów baz danych. Dostępne są regulacje dotyczące stosowania prywatnych nośników danych lub użytkowanie prywatnych nośników danych jest zabronione. Dostępne są wiążące regulacje dotyczące dostępu do danych dla potrzeb zewnętrznych prac konserwacyjnych, konserwacji zdalnej i pracy zdalnej. Niszczenie/utylizowanie dokumentów i nośników danych (np. niszczarka, pojemnik na poufne dokumenty) jest realizowane zgodnie z przepisami o ochronie danych osobowych przez wiarygodną firmę utylizacyjną.

Koncepcja ról/uprawnień jest regularnie dostosowywana do zmieniających się struktur organizacyjnych prac (np. nowe role), a przydzielone role/uprawnienia są regularnie sprawdzane (np. przez przełożonych) i w razie potrzeby dostosowywane lub odbierane. Regularnie prowadzona jest centralna kontrola w zakresie przypisanych profili standardowych. Każdy dostęp modyfikujący (zapis, usunięcie) jest protokołowany, a wygenerowane pliki protokołu są przechowywane przez odpowiedni okres (minimum 90 dni) i (wyrywkowo) sprawdzane.

Jako ogólne środki do zabezpieczenia przekazywania danych stosuje się różne środki standardowe:

Osoby zajmujące się przekazywaniem danych są zapoznawane uprzednio z wymaganymi środkami bezpieczeństwa. Krąg odbiorców jest ustalany z góry w celu umożliwienia odpowiedniej kontroli (uwierzytelniania). Całość procesu przekazywania danych jest ustalona i dokumentowana, a realizacja konkretnego przekazywania danych jest protokołowana lub dokumentowana (np. potwierdzenie odbioru, pokwitowanie). Osoby zajmujące się przekazywaniem danych wykonują najpierw weryfikację zasadności, kompletności i zgodności ze stanem faktycznym.

Przed zrealizowaniem konkretnego przesyłu danych następuje weryfikacja adresu odbioru (np. adres e-mail). Przesyłanie danych poprzez Internet odbywa się w formie szyfrowanej (np. szyfrowanie pliku). W miarę możliwości technicznych integralność przesyłanych danych jest gwarantowana poprzez zastosowanie sygnatury (sygnatura cyfrowa). Elektroniczne potwierdzenia odbioru są archiwizowane w odpowiedniej formie. Niepożądanej transmisji danych w Internecie zapobiega się poprzez zastosowanie odpowiednich technologii (np. proxy, zapora ogniowa).

Ponadto jako środki w celu realizacji nakazu rozdziału stosuje się następujące środki standardowe:

Dostępne są wiążące regulacje dotyczące ścisłego przeznaczenia przetwarzania danych w celu spełnienia nakazu rozdziału. Dane pozyskiwane w określonych celach są zapisywane oddzielnie od danych pozyskiwanych w innych celach. Stosowane systemy IT pozwalają na oddzielne zapisywanie danych (poprzez obsługę wielu klientów lub koncepcje dostępu). Dane są rozdzielane w systemach testowych i produkcyjnych. W przypadku danych pseudonimizowanych zapisuje się lub przechowuje oddzielnie klucz umożliwiający ponowne zidentyfikowanie danych. W przypadku przetwarzania danych dotyczących zlecenia lub przeniesienia funkcji

następuje oddzielne przetwarzanie danych różnych zleceniodawców u Zleceniobiorcy. Istniejące koncepcje ról/uprawnień umożliwiają logiczny rozdział przetwarzanych danych poprzez swoją konstrukcję.

4. Gwarancja integralności

Jako środki do realizacji protokołowania wprowadzanych danych stosuje się różne środki standardowe:

Protokołowane są zmiany uprawnień dostępu oraz wszystkie czynności administracyjne. Protokołowany jest dostęp z zapisem (wprowadzanie, zmiany, usuwanie danych) i zmiany w polach danych (np. zawartość nowo wprowadzonego lub zmienionego rekordu danych). Protokołowane są przesyły (np. pobieranie) i logowania.

Wykorzystywane dokumenty rejestracyjne są dokumentowane i archiwizowane w celu monitorowania wprowadzania danych. Informacje są protokołowane z podaniem daty i godziny, użytkownika, rodzaju działania, aplikacji i numeru porządkowego rekordu danych. Ustawienia protokołowania są dokumentowane.

Dostęp do plików protokołu jest możliwy wyłącznie na zasadzie odczytu. Grono osób uprawnionych do dostępu do plików protokołu jest ściśle ograniczone (np. do administratora, osoby odpowiedzialnej za ochronę danych, rewidenta). Pliki protokołu są przechowywane przez ustalony okres (np. 1 dni), a następnie usuwane z zachowaniem wymogów ochrony danych. Pliki protokołu są regularnie analizowane w sposób automatyczny. Analizy plików protokołu są w miarę możliwości sporządzane w formie pseudonimizowanej.

5. Gwarancja dostępności

Architektura jest z natury zabezpieczona przed utratą danych poprzez wewnętrzne mechanizmy replikacji w obrębie platformy AWS. Ponadto jako środki do zabezpieczenia obiektów stosuje się następujące środki standardowe AWS:

Stosowane są środki ochrony przeciwpożarowej (np. drzwi przeciwpożarowe, czujniki dymu, ściany przeciwpożarowe, zakaz palenia). Instalacje komputerowe są chronione przed zalaniem (np. serwerownia na pierwszym piętrze, czujnik wody). Stosowane są środki ochrony przed wstrząsami (np. serwerownia z dala od dróg szybkiego ruchu, torów kolejowych, maszynowni). Urządzenia komputerowe są chronione przed oddziaływaniem pól elektromagnetycznych (np. płyty stalowe w ścianach zewnętrznych). Stosowane są środki ochrony przed aktami wandalizmu i kradzieżą (por. kontrola dostępu). Urządzenia komputerowe znajdują się w pomieszczeniach klimatyzowanych (temperatura i wilgotność powietrza jest regulowana przez klimatyzację). Urządzenia komputerowe są chronione przed przepięciem poprzez zabezpieczenia przeciwprzepięciowe. Stosowane są środki w celu zapewnienia bezawaryjnego i ciągłego zasilania elektrycznego (np. urządzenia UPS, zespoły prądotwórcze).

Bazy danych są regularnie zabezpieczane w formie kopii zapasowych w obrębie platformy AWS. Koncepcja kopii bezpieczeństwa jest udokumentowana i jest regularnie weryfikowana oraz aktualizowana. Nośniki z kopiami bezpieczeństwa są chronione przed dostępem osób nieupoważnionych. Stosowane programy do sporządzania kopii bezpieczeństwa spełniają aktualne standardy jakości i są w tym zakresie regularnie aktualizowane.

Zapewnione jest redundantne centrum danych (oddalone od miejsca przetwarzania), które w razie awarii jest w stanie kontynuować przetwarzanie danych. Różnorodne środki kontroli dostępności są udokumentowane w planie zarządzania awaryjnego AWS.

Przed przekazaniem zlecenia na przetwarzanie danych Zleceniobiorca jest starannie sprawdzany według ustalonych kryteriów (środki techniczne i organizacyjne). W tym celu wymagane jest zwłaszcza szczegółowe przedstawienie technicznych/organizacyjnych środków ochrony danych stosowanych przez Zleceniobiorcę (udzielenie odpowiedzi na zbiór pytań lub koncepcja ochrony danych), które jest weryfikowane. W zależności od ilości i wrażliwości przetwarzanych danych weryfikacja ta może być również wykonywana w siedzibie Zleceniobiorcy. Przy wyborze zleceniobiorców uwzględniane są odpowiednie certyfikaty (np. ISO 27001). Stwierdzenie adekwatności Zleceniobiorcy jest dokumentowane w stosownej i zrozumiałej formie.

W celu ustanowienia relacji stron zawierana jest umowa o przetwarzanie danych dotyczących zlecenia pomiędzy Zleceniodawcą a Zleceniobiorcą. Umowa ta określa szczegółowo i w formie pisemnej zakres kompetencji i odpowiedzialności oraz obowiązki obu stron. Jeżeli siedziba zaangażowanego usługodawcy znajduje się poza terytorium UE lub EOG, stosuje się standardowe klauzule umowne UE. Zgodnie z uregulowaniami umownymi przetwarzanie danych przez Zleceniobiorcę może być realizowane wyłącznie w ramach wytycznych udzielonych przez Zleceniodawcę. Zleceniobiorca jest zobowiązany do niezwłocznego powiadomienia Zleceniodawcy, jeżeli którekolwiek z wytycznych udzielonych przez Zleceniodawcę są zdaniem Zleceniobiorcy niezgodne z przepisami o ochronie danych. W celu zachowania praw podmiotów danych uzgadnia się w umowie o przetwarzanie danych dotyczących zlecenia, że Zleceniobiorca jest zobowiązany do zapewnienia Zleceniodawcy odpowiedniego wsparcia, jeżeli jest to wymagane np. w zakresie udzielenia informacji dla podmiotów danych.

W dalszym przebiegu przetwarzania danych dotyczących zlecenia Zleceniodawca kontroluje rezultaty prac Zleceniobiorcy pod względem formalnym i merytorycznym. Przestrzeganie środków technicznych i organizacyjnych zastosowanych u Zleceniobiorcy jest regularnie weryfikowane. Do tych celów służy głównie przedstawienie aktualnych atestów lub odpowiednich certyfikatów bądź dokument potwierdzający przeprowadzenie audytu bezpieczeństwa IT lub audytu ochrony danych. W przypadku korzystania z usług podwykonawców strony uzgadniają w umowie zapewnienia odpowiedniej kontroli nad ich działaniami.

6. Gwarancja wytrzymałości systemów

Infrastruktura chmury AWS została stworzona jako jedno z najbardziej elastycznych i bezpiecznych środowisk chmury obliczeniowej. Jej koncepcja została opracowana z myślą o optymalizacji dostępności przy całkowitym rozdziale klientów. Infrastruktura ta oferuje nadzwyczaj skalowalną, wysoce stabilną platformę, która w razie potrzeby umożliwia klientom szybkie i bezpieczne przekazywanie aplikacji i treści na całym świecie. Usługi AWS są o tyle niezależne od treści, że oferują ten sam wysoki poziom bezpieczeństwa dla wszystkich klientów, niezależnie od rodzaju treści lub od regionu geograficznego, w którym treści są zapisywane.

Centra danych AWS o wysokim poziomie bezpieczeństwa światowej klasy wykorzystują nowoczesne elektroniczne środki nadzoru i systemy wielostopniowej kontroli dostępu. Centra danych są obsługiwane całodobowo przez wykwalifikowany personel ds. zabezpieczeń, a dostęp jest udzielany ściśle według zasady minimalnych uprawnień oraz wyłącznie w celu administrowania systemem.

7. Procedura odzyskiwania dostępności danych osobowych po wystąpieniu zdarzenia fizycznego lub technicznego

Centra danych AWS są budowane w klastrach w różnych regionach świata. Wszystkie centra danych są online i obsługują klientów; żadne centrum danych nie jest odłączone. W przypadku awarii automatyczne procesy odsuwają przepływ danych klientów od uszkodzonych obszarów. Kluczowe aplikacje są udostępniane w konfiguracji N+1, aby w razie awarii centrum danych dostępne były zasoby wystarczające do rozłożenia przepływu danych z równomiernym obciążeniem na pozostałe lokalizacje.

AWS oferuje elastyczność umieszczania wystąpień i zapisywania danych w obrębie wielu regionów geograficznych oraz wielu stref dostępności w ramach poszczególnych regionów. Każda strefa dostępności została stworzona jako niezależna strefa na wypadek awarii. Oznacza to, że strefy dostępności są fizycznie rozłożone w obrębie typowego regionu miejskiego i znajdują się np. na terenach o niskim ryzyku zalewowym (w zależności od regionu dostępne są różne kategorie stref zalewowych). Dodatkowo do własnego ciągłego zasilania i generatorów awaryjnych, wszystkie strefy dostępności są zasilane z różnych sieci energetycznych przez niezależnych dostawców energii w celu zminimalizowania pojedynczych punktów podatności na awarię. Wszystkie strefy dostępności są powiązane w sposób redundantny z wieloma dostawcami Tier-1-Transit.

Zespół Amazon ds. zarządzania zdarzeniami stosuje branżowe procesy diagnostyczne w celu przyspieszania usuwania skutków zdarzeń krytycznych dla przedsiębiorstwa. Personel zakładowy zapewnia ciągłość obsady w trybie całodobowym, siedem dni w tygodni i 365 dni w roku, w celu wykrywania zakłóceń oraz eliminowania ich skutków.

8. Procedura regularnej weryfikacji, analizy i oceny skuteczności środków technicznych i organizacyjnych

Wytyczne i instrukcje dostępne w firmie lub wdrożone standardy bezpieczeństwa informacji są stosowane również w odniesieniu do wdrożenia i obsługi platformy RIO. Dostępne są zakładowe stanowiska ds. ochrony danych i bezpieczeństwa informacji (osoba odpowiedzialna za ochronę danych osobowych i specjalista ds. bezpieczeństwa informacji). Osoby zatrudnione są zobowiązane do zachowania tajemnicy danych oraz są informowane o środkach bezpieczeństwa danych lub zabezpieczeniach IT poprzez broszury, ulotki, wskazówki w Intranecie itp.

Procesy wewnętrzne są sprawdzane pod kątem przestrzegania technicznych i organizacyjnych środków zapewnienia bezpieczeństwa danych poprzez weryfikację, bezpieczeństwo informacji i ochronę danych.

Procesy przetwarzania i środki bezpieczeństwa danych są udokumentowane w spisie działań dotyczących przetwarzania danych. Skuteczność środków jest poddawana regularnej weryfikacji (wewnętrznej i zewnętrznej).