Umowa o przetwarzaniu danych
w oparciu o standardowe klauzule umowne WE
pomiędzy administratorami i podmiotami przetwarzającymi w obrębie UE / EOG
na podstawie art. 28 rozporządzenia (UE) 2016/679 (RODO)

SEKCJA I

Klauzula 1 / Cel i zakres

(a) Celem niniejych standardowych klauzul umownych („klauzule") jest zapewnienie przestrzegania art. 28 ust. 3 i 4 rozporządzenia 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.

(b) Administratorzy i podmioty przetwarzające wymienieni w załączniku I uzgodnili niniejsze klauzule w celu zapewnienia przestrzegania art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679.

(c) Niniejsze klauzule mają zastosowanie do przetwarzania danych osobowych określonego w załączniku II.

(d) Załączniki I–IV stanowią integralną część klauzul.

(e) Niniejsze klauzule pozostają bez uszczerbku dla obowiązków, którym podlega administrator danych na mocy rozporządzenia (UE) 2016/679.

(f) Niniejsze klauzule same w sobie nie zapewniają wypełnienia obowiązków związanych z międzynarodowym przekazywaniem danych zgodnie z rozdziałem V rozporządzenia (UE) 2016/679.

Klauzula 2 / Niezmienność klauzul

(a) Strony zobowiązują się nie zmieniać klauzul z wyjątkiem dodawania informacji do załączników lub aktualizowania zawartych w nich informacji.

(b) Postanowienie to nie uniemożliwia stronom umieszczania standardowych klauzul umownych określonych w niniejszych klauzulach w treści umowy o szerszym zakresie ani dodawania innych klauzul lub dodatkowych zabezpieczeń, pod warunkiem że nie będą one bezpośrednio lub pośrednio sprzeczne z klauzulami umownymi ani nie będą naruszały podstawowych praw lub wolności osób, których dane dotyczą.

Klauzula 3 / Wykładnia

(a) Jeżeli w niniejszych klauzulach użyto terminów zdefiniowanych odpowiednio w rozporządzeniu (UE) 2016/679, terminy te mają takie samo znaczenie jak w tym rozporządzeniu.

(b) Niniejsze klauzule odczytuje się i interpretuje w świetle odpowiednio przepisów rozporządzenia (UE) 2016/679.

(c) Niniejszych klauzul nie interpretuje się w sposób sprzeczny z prawami i obowiązkami przewidzianymi w rozporządzeniu (UE) 2016/679 ani w sposób naruszający podstawowe prawa lub wolności osób, których dane dotyczą.

Klauzula 4 / Hierarchia

W razie sprzeczności między niniejszymi klauzulami a postanowieniami powiązanych umów między stronami istniejących w chwili uzgadniania niniejszych klauzul lub zawartych po ich uzgodnieniu, pierwszeństwo mają niniejsze klauzule.

Klauzula 5 – fakultatywna / Klauzula przystąpienia

(a) Każdy podmiot niebędący stroną niniejszych klauzul może za zgodą wszystkich stron przystąpić do niniejszych klauzul jako administrator lub podmiot przetwarzający w dowolnym czasie, wypełniając załączniki i podpisując załącznik I.

(b) Po wypełnieniu i podpisaniu załączników wymienionych w lit. a) podmiot przystępujący jest traktowany jako strona niniejszych klauzul i ma prawa i obowiązki administratora lub podmiotu przetwarzającego, zgodnie z rolą nadaną mu w załączniku I.

(c) Przed przystąpieniem do niniejszych klauzul jako ich strona podmiot przystępujący nie ma żadnych praw ani obowiązków wynikających z niniejszych klauzul.

SEKCJA II / Opis przetwarzania

Klauzula 6 / Opis przetwarzania

Szczegóły dotyczące operacji przetwarzania, w szczególności kategorie danych osobowych i cele, dla których dane osobowe są przetwarzane w imieniu administratora, określono w załączniku II.

Klauzula 7 / Obowiązki stron

7.1. Polecenia

(a) Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny. Administrator może wydawać kolejne polecenia przez cały okres przetwarzania danych osobowych. Polecenia te są zawsze dokumentowane.

(b) Podmiot przetwarzający bezzwłocznie powiadamia administratora, jeżeli w opinii podmiotu przetwarzającego polecenie wydane przez administratora narusza rozporządzenie (UE) 2016/679 lub obowiązujące przepisy Unii lub państwa członkowskiego o ochronie danych.

7.2. Ograniczenie celu

Podmiot przetwarzający przetwarza dane osobowe wyłącznie w konkretnym celu lub celach przetwarzania, określonych w załączniku II, chyba że otrzyma dalsze polecenia od administratora.

7.3. Czas trwania przetwarzania danych osobowych

Przetwarzanie przez podmiot przetwarzający odbywa się wyłącznie przez okres określony w załączniku II.

7.4. Bezpieczeństwo przetwarzania

(a) W celu zapewnienia bezpieczeństwa danych osobowych podmiot przetwarzający wdraża co najmniej środki techniczne i organizacyjne określone w załączniku III. Zapewnienie bezpieczeństwa danych obejmuje ochronę danych przed naruszeniem bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych (naruszenie ochrony danych osobowych). Oceniając odpowiedni poziom bezpieczeństwa, strony należycie uwzględniają stan wiedzy technicznej, koszty wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz związane z tym ryzyko dla osób, których dane dotyczą.

(b) Podmiot przetwarzający udziela członkom swojego personelu dostępu do danych osobowych podlegających przetwarzaniu jedynie w zakresie bezwzględnie niezbędnym do wykonania umowy, zarządzania nią i jej monitorowania. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania otrzymanych danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

7.5. Dane wrażliwe

Jeżeli przetwarzanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne do celów jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby, bądź dane dotyczące wyroków skazujących i czynów zabronionych („dane wrażliwe”), podmiot przetwarzający stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia.

7.6. Dokumentacja i zgodność

(a) Strony są w stanie wykazać zgodność z niniejszymi klauzulami.

(b) Podmiot przetwarzający niezwłocznie i odpowiednio rozpatruje zapytania administratora dotyczące przetwarzania danych zgodnie z niniejszymi klauzulami.

(c) Podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków, które są określone w niniejszych klauzulach i wynikają bezpośrednio z rozporządzenia (UE) 2016/679. Na wniosek administratora podmiot przetwarzający zezwala również na audyty czynności przetwarzania objętych niniejszymi klauzulami i uczestniczy w tych audytach. Audyty te przeprowadza się w rozsądnych odstępach czasu lub jeżeli istnieją przesłanki wskazujące na niezgodność. Podejmując decyzję w sprawie przeglądu lub audytu, administrator może wziąć pod uwagę odpowiednie certyfikaty, jakie ma podmiot przetwarzający.

(d) Administrator może przeprowadzić audyt samodzielnie lub upoważnić do jego przeprowadzenia niezależnego audytora. Audyty mogą również obejmować inspekcje w pomieszczeniach lub obiektach fizycznych podmiotu przetwarzającego. Audyty te przeprowadza się, informując o nich, w stosownych przypadkach, z odpowiednim wyprzedzeniem.

(e) Na wniosek właściwego(-ych) organu(-ów) nadzorczego(-ych) strony udostępniają mu (im) informacje, o których mowa w niniejszej klauzuli, w tym wyniki wszelkich audytów.

7.7. Korzystanie z usług podmiotów podprzetwarzających

(a) Podmiot przetwarzający posiada ogólne upoważnienie administratora danych do angażowania podwykonawcy/-ów przetwarzania z uzgodnionej listy. Podmiot przetwarzający informuje administratora pisemnie o wszelkich zamierzonych zmianach w tym wykazie poprzez dodanie lub zastąpienie podwykonawców przetwarzania z wyprzedzeniem co najmniej 30 dni, dając tym samym administratorowi wystarczający czas na zgłoszenie sprzeciwu wobec takich zmian przed zaangażowaniem danego/-ych podwykonawcy/-ów. Podmiot przetwarzający przekazuje administratorowi informacje niezbędne do umożliwienia mu skorzystania z prawa do sprzeciwu.

(b) Jeżeli podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu administratora), dokonuje tego w drodze umowy, która nakłada na podmiot podprzetwarzający zasadniczo takie same obowiązki w zakresie ochrony danych jak obowiązki nałożone na podmiot przetwarzający dane zgodnie z niniejszymi klauzulami. Podmiot przetwarzający zapewnia, aby podmiot podprzetwarzający wypełniał obowiązki, którym podlega podmiot przetwarzający na mocy niniejszych klauzul oraz rozporządzenia (UE) 2016/679.

(c) Na wniosek administratora podmiot przetwarzający przekazuje administratorowi kopię umowy, jaką zawarł z podmiotem podprzetwarzającym, a w razie wprowadzenia zmian przekazuje administratorowi jej zaktualizowaną wersję. W zakresie niezbędnym do ochrony tajemnicy handlowej lub innych informacji poufnych, w tym danych osobowych, podmiot przetwarzający może utajnić tekst umowy przed jej udostępnieniem.

(d) Podmiot przetwarzający pozostaje w pełni odpowiedzialny przed administratorem za wykonanie obowiązków podmiotu podprzetwarzającego zgodnie z jego umową z podmiotem przetwarzającym. Podmiot przetwarzający powiadamia administratora o każdym przypadku niewywiązania się przez podmiot podprzetwarzający z jego zobowiązań umownych.

(e) Podmiot przetwarzający uzgadnia z podmiotem podprzetwarzającym klauzulę dotyczącą beneficjenta będącego osobą trzecią, zgodnie z którą to klauzulą – jeżeli podmiot przetwarzający przestanie istnieć faktycznie lub formalnie lub stanie się niewypłacalny – administrator ma prawo rozwiązać umowę z podmiotem podprzetwarzającym i nakazać mu usunięcie lub zwrot danych osobowych.

7.8. Międzynarodowe przekazywanie danych

(a) Wszelkie przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej przez podmiot przetwarzający odbywa się wyłącznie na udokumentowane polecenie administratora lub w celu spełnienia szczególnego wymogu na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega podmiot przetwarzający, i odbywa się zgodnie z rozdziałem V rozporządzenia (UE) 2016/679.

(b) Jeżeli zgodnie z klauzulą 7.7 podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu administratora), które wiążą się z przekazywaniem danych osobowych w rozumieniu rozdziału V rozporządzenia (UE) 2016/679, administrator wyraża zgodę na to, by podmioty te mogły zapewnić zgodność z rozdziałem V rozporządzenia (UE) 2016/679 za pomocą standardowych klauzul umownych przyjętych przez Komisję zgodnie z art. 46 ust. 2 rozporządzenia (UE) 2016/679, pod warunkiem że spełnione są warunki stosowania tych standardowych klauzul umownych.

Klauzula 8 / Pomoc dla administratora

(a) Podmiot przetwarzający niezwłocznie zawiadamia administratora o każdym wniosku otrzymanym od osoby, której dane dotyczą. Podmiot przetwarzający nie odpowiada na taki wniosek samodzielnie, chyba że administrator wyraził na to zgodę.

(b) Podmiot przetwarzający pomaga administratorowi w wypełnianiu jego obowiązków dotyczących udzielania odpowiedzi na wnioski osób, których dane dotyczą, o skorzystanie z przysługujących im praw, z uwzględnieniem charakteru przetwarzania. Wypełniając swoje obowiązki zgodnie z lit. a) i b), podmiot przetwarzający stosuje się do poleceń administratora.

(c) Oprócz spoczywającego na podmiocie przetwarzającym obowiązku pomagania administratorowi zgodnie z klauzulą 8 lit. b) podmiot przetwarzający pomaga mu ponadto w zapewnieniu wypełniania następujących obowiązków, z uwzględnieniem charakteru przetwarzania danych oraz informacji, którymi dysponuje podmiot przetwarzający:

(1) obowiązek przeprowadzenia oceny wpływu planowanych operacji przetwarzania na ochronę danych osobowych („ocena skutków dla ochrony danych"), jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych;

(2) obowiązek skonsultowania się z właściwym(-i) organem(-ami) nadzorczym(-i) przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu jego ograniczenia;

(3) obowiązek zapewnienia prawidłowości i aktualności danych osobowych poprzez niezwłoczne poinformowanie administratora, jeżeli podmiot przetwarzający stwierdzi, że przetwarzane przez niego dane osobowe są nieprawidłowe lub nieaktualne;

(4) obowiązki określone w art. 32 rozporządzenia (UE) 2016/679

(d) Strony określają w załączniku III odpowiednie środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający jest zobowiązany pomagać administratorowi w stosowaniu niniejszej klauzuli, jak również zakres wymaganej pomocy.

Klauzula 9 / Zgłaszanie naruszenia ochrony danych osobowych

W przypadku naruszenia ochrony danych osobowych podmiot przetwarzający współpracuje z administratorem i pomaga mu w wypełnianiu jego obowiązków wynikających z art. 33 i 34 rozporządzenia (UE) 2016/679, z uwzględnieniem charakteru przetwarzania i informacji, którymi dysponuje podmiot przetwarzający.

9.1 Naruszenie ochrony danych dotyczące danych przetwarzanych przez administratora

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez administratora podmiot przetwarzający wspomaga administratora:

(a) przy zgłaszaniu naruszenia ochrony danych osobowych właściwemu(-ym) organowi(-om) nadzorczemu(-ym) niezwłocznie po tym, jak administrator dowiedział się o naruszeniu, w stosownych przypadkach/(chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych);

(b) przy uzyskiwaniu następujących informacji, które zgodnie z art. 33 ust. 3 rozporządzenia (UE) 2016/679 powinny być zawarte w zgłoszeniu administratora i obejmować co najmniej:

(1) charakter danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

(2) możliwe konsekwencje naruszenia ochrony danych osobowych;

(3) środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki;

(c) przy wypełnianiu – zgodnie z art. 34 rozporządzenia (UE) 2016/679 – obowiązku zawiadomienia bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.

9.2 Naruszenie ochrony danych dotyczące danych przetwarzanych przez podmiot przetwarzający

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez podmiot przetwarzający podmiot przetwarzający zgłasza naruszenie administratorowi niezwłocznie po tym, jak dowiedział się o naruszeniu. Zgłoszenie to powinno zawierać co najmniej:

(a) opis charakteru naruszenia (w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz wpisów danych, których dotyczy naruszenie);

(b) punktu kontaktowego, w którym można uzyskać więcej informacji na temat naruszenia ochrony danych osobowych;

(c) wskazanie prawdopodobnych konsekwencji naruszenia oraz środków, które zostały lub mają zostać wprowadzone w celu zaradzenia naruszeniu, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki.

Strony określają w załączniku III wszystkie inne elementy, które ma przedstawić podmiot przetwarzający, wspomagając administratora w wypełnianiu jego obowiązków określonych w art. 33 i 34 rozporządzenia (UE) 2016/679

SEKCJA III / POSTANOWIENIA KOŃCOWE

Klauzula 10 / Naruszenie klauzul i rozwiązanie umowy

(a) Bez uszczerbku dla przepisów rozporządzenia (UE) 2016/679, w przypadku gdy podmiot przetwarzający narusza swoje obowiązki wynikające z niniejszych klauzul, administrator może polecić mu, by zawiesił przetwarzanie danych osobowych do czasu, gdy podmiot przetwarzający zapewni zgodność z niniejszymi klauzulami, lub umowa ulega rozwiązaniu. Podmiot przetwarzający niezwłocznie zawiadamia administratora, jeżeli z jakiegokolwiek powodu nie jest w stanie zastosować się do niniejszych klauzul.

(b) Administrator jest uprawniony do rozwiązania umowy w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli:

(1) administrator zawiesił przetwarzanie danych osobowych przez podmiot przetwarzający zgodnie z lit. a) i jeżeli zgodność z niniejszymi klauzulami nie zostanie przywrócona w rozsądnym terminie, a w każdym razie w terminie jednego miesiąca od zawieszenia;

(2) podmiot przetwarzający poważnie lub stale narusza niniejsze klauzule lub swoje obowiązki wynikające z rozporządzenia (UE) 2016/679;

(3) podmiot przetwarzający nie stosuje się do wiążącej decyzji właściwego sądu lub właściwego(-ych) organu(-ów) nadzorczego(-ych) dotyczącej jego obowiązków wynikających z niniejszych klauzul lub z rozporządzenia (UE) 2016/679.

(c) Podmiot przetwarzający ma prawo rozwiązać umowę w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli po zawiadomieniu administratora o tym, że jego polecenie narusza obowiązujące wymogi prawne zgodnie z klauzulą 7.1 lit. b), administrator nalega na wypełnienie polecenia.

(d) Po rozwiązaniu umowy podmiot przetwarzający, zależnie od decyzji administratora, usuwa wszystkie dane osobowe przetwarzane w imieniu administratora i poświadcza administratorowi, że tego dokonał, lub zwraca administratorowi wszystkie dane osobowe i usuwa istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. Podmiot przetwarzający zapewnia przestrzeganie niniejszych klauzul do czasu usunięcia lub zwrotu danych.

ZAŁĄCZNIK I / WYKAZ STRON

Administrator (administratorzy): *[dane identyfikacyjne i kontaktowe administratora (administratorów) oraz, w stosownych przypadkach, inspektora ochrony danych wyznaczonego przez administratora]*

Imię i nazwisko/ nazwa:	
Adres:	
Osoba kontaktowa **(Imię i nazwisko, stanowisko i dane kontaktowe):**	
Data dostępu:	
Podpis:	

Podmiot przetwarzający (podmioty przetwarzające*): [dane identyfikacyjne i kontaktowe podmiotu przetwarzającego (podmiotów przetwarzających) oraz, w stosownych przypadkach, inspektora ochrony danych wyznaczonego przez podmiot przetwarzający]*

Imię i nazwisko/ nazwa:	**Bridgestone Mobility Solutions B.V.**
Adres:	Beethovenstraat 503, 1083 HK Amsterdam, Holandia
Osoba kontaktowa **(Imię i nazwisko, stanowisko i dane kontaktowe):**	Loreto Reguera Bridgestone West Chief Privacy Officer & DPO digitaltrust@webfleet.com
Data dostępu:	
(Imię i nazwisko, stanowisko i dane kontaktowe upoważnionego przedstawiciela): **Podpis:**	_____ _____

ZAŁĄCZNIK II / OPIS PRZETWARZANIA

Kategorie podmiotów danych, których dane osobowe są przetwarzane

Podmioty:

Kierowcy

- Użytkownicy Serwisu WEBFLEET, dostępnego za pośrednictwem Internetu pod adresem **www.webfleet.com**

Kategorie przetwarzanych danych osobowych

Dane zarządzane przez użytkownika i tworzone treści:

Dane	**Opis**
Adresy	Dane geolokalizacyjne, adresy wysyłkowe i punkty orientacyjne wykorzystywane przez menedżerów floty
Dane administratora	Imię i nazwisko administratora, adres e-mail, adres IP, numer telefonu (jeśli podano)
Dane kierowcy	Nazwisko kierowcy, adres, adres e-mail, licencja i dane kontaktowe
Zlecenia	Dane dotyczące pracy kierowców
Wiadomości tekstowe	Wiadomości wymieniane pomiędzy kierownikiem floty a kierowcą poprzez terminale kierowcy
Dane pojazdu	Indywidualne specyfikacje pojazdu, dane z gelokacji i czujników, dodatkowe dane telematyczne, w tym rejestracja, numer VIN lub tablica rejestracyjna, przejechany dystans, czas jazdy, pora dnia, prędkość pojazdu i silnika, obciążenie i temperatura silnika, dane przyczepy, nagrania z kamer (do wewnątrz i na zewnątrz), ciśnienie w oponach, zachowanie kierowcy, manewry hamowania/skręcania/przyspieszania, napięcie akumulatora, protokoły danych o wypadkach na 45 sekund przed i 15 sekund po wypadku; urządzenia pojazdu, czujniki, dane diagnostyczne związane z serwisem, dane z tachografu. Przetwarzanie dodatkowych danych zależy od tego, czy te typy danych zostały udostępnione przez Kontrolera Procesorowi, w oparciu o wybrany rodzaj subskrypcji
Obszary	Definicje geostrefy w celu określenia obszarów o pożądanej lub niepożądanej pozycji pojazdu
Trasy	Wstępnie zdefiniowane trasy przejazdu, zlecenia, planowane trasy na terminalach kierowcy
Raporty (dokumenty)	Specyfikacje raportów i dokumenty wynikowe

Dane transakcyjne:

Dane	**Opis**
przyspieszenie (boczne)	Zdarzenia związane z ostrym hamowaniem, pokonywaniem zakrętów i startami w wyścigach
Dane CAN/OBD	Sygnały z interfejsu Controller Area Network (CAN) lub interfejsu diagnostyki pokładowej (OBD) pojazdu jako wskaźniki usterek, przewidywanie konserwacji, monitorowanie drzwi, poziom paliwa itp.
Zmiany w zapłonie	Czy i kiedy zapłon jest włączany i wyłączany
pozycje	Aktualna lokalizacja pojazdu za pomocą urządzenia LINK
Dane z tachografu	Godziny pracy kierowcy w przypadku pojazdów ciężarowych i pojazdów przewożących pasażerów zebrane przez tachografy cyfrowe
Monitorowanie urządzeń śledzących	Ruch pojazdu z wyłączonym zapłonem (holowanie, kradzież), odłączenie zasilania, ekranowanie urządzenia śledzącego.

ślady	Sekwencja spójnych pozycji
Kody usterek	Wskaźniki usterek pobrane z magistrali FMS pojazdów ciężarowych lub OBD

Dane zbiorcze:

Dane	Opis
KPIs	Zagregowane wskaźniki jazdy i zachowania wykorzystywane w OptiDrive score
Statystyki pojazdu	Dane dotyczące zdarzeń drogowych i śladu węglowego zagregowane w czasie
Statystyki kierowcy	Zachowanie kierowcy zagregowane w czasie
Statystyki czasu pracy	Wjazd i wyjazd kierowcy/współkierowcy
Książka jazd	Dziennik pokładowy kierowcy
Karty paliwowe	Zakup paliwa za pomocą kart płatniczych

Przetwarzanie pomocnicze:

Informacje o używanym urządzeniu, lokalizacjach, trasach, miejscach docelowych i zapytaniach wyszukiwania. Informacje te są wykorzystywane do diagnostyki technicznej, wykrywania oszustw i nadużyć, tworzenia raportów użytkowania oraz ulepszania naszych usług. Dane te nie pozwalają WEBFLEET lub naszym Podwykonawcom Przetwarzania na identyfikację klienta lub jego kierowców i mają charakter zbiorczy.

Przetwarzane danych wrażliwych

Brak

Charakter przetwarzania danych

W trakcie świadczenia Usług i Produktów WEBFLEET na rzecz Klienta zgodnie z Warunkami Umowy WEBFLEET

Cel(e), dla których dane osobowe są przetwarzane w imieniu administratora

Świadczenie Usługi WEBFLEET opisanej w Warunkach WEBFLEET, w tym między innymi Przetwarzanie (i) śledzenia pojazdu; (ii) zachowania kierowcy i oszczędności paliwa; (iii) dwukierunkowej komunikacji z kierowcą; (iv) informacji o tachografie i pozostałym czasie jazdy; (v) obszernego raportowania; (vi) integracji rozwiązań stron trzecich / integracji biznesowej; (vii) danych z kamery samochodowej.

Czas trwania przetwarzania

Dane transakcyjne:

Dane	Czas retencji
Stanowiska	90 dni (Francja: 60 dni)
Ścieżki	
Dane CAN/OBD	
Zmiany w zapłonie	
Stany zamówień	
Kody usterek	
Przyspieszenie (boczne)	
Monitorowanie urządzenia śledzącego	
Zmiany stanu pracy	40 dni
Dane z tachografu	2 lata

Dane zarządzane przez użytkownika i tworzone treści:

Dane	Czas retencji
Wiadomości tekstowe	90 dni (Francja: 60 dni)
Zarchiwizowane raporty	1 miesiąc do 36 miesięcy

Dane zbiorcze:

Dane	Czas retencji
KPIs	2 pełne lata + rok bieżący
Statystyka pojazdów	
Statystyka kierowców	
Statystyka czasu pracy	
Dziennik pokładowy	
Karty paliwowe	

Należy pamiętać, *że klient może zażądać usunięcia danych, które były przetwarzane w twoim imieniu, kontaktując się z naszym zespołem wsparcia technicznego telefonicznie lub poprzez pocztę elektroniczną.*

Dane gromadzone na potrzeby raportowania wyjazdów fiskalnych lub raportowania czasu pracy, takie jak zarządzanie tachografami, mogą podlegać innym odpowiednim przepisom. Administrator danych ma obowiązek ustalić, czy przepisy te mogą uniemożliwić administratorowi danych zaangażowanie się w usuwanie danych

W przypadku przetwarzania przez podwykonawców przetwarzania/podmioty przetwarzające należy również określić przedmiot, charakter i czas trwania przetwarzania	Przetwarzanie jest opisane w liście Podwykonawców Przetwarzania i jest związane ze świadczeniem Usługi i Produktów WEBFLEET. Czas trwania przetwarzania jest taki sam jak czas trwania przetwarzania przez Podmiot Przetwarzający

ZAŁĄCZNIK III / ŚRODKI TECHNICZNE I ORGANIZACYJNE, W TYM ŚRODKI TECHNICZNE I ORGANIZACYJNE W CELU ZAPEWNIENIA BEZPIECZEŃSTWA DANYCH

Podmiot przetwarzający utrzymuje certyfikat ISO/IEC 27001, który obejmuje poniższe środki techniczne i organizacyjne i jest dostępny na żądanie

Poufność

Art. 32 (1) (b) RODO

(i) Kontrola dostępu (budynek | biura | centrum danych)

Zapobieganie nieuprawnionemu dostępowi do systemów przetwarzania danych, w których przetwarzane są dane osobowe

- ☒ System alarmowy
- ☒ Automatyczny system kontroli dostępu
- ☒ Czujniki fotoelektryczne / Czujniki ruchu
- ☒ Zarządzanie kluczami (wydawanie kluczy itp.)
- ☒ Rejestrowanie odwiedzających
- ☒ Staranny dobór pracowników ochrony
- ☒ Ochrona szybów budowlanych
- ☒ Karta z chipem / system zamykania transponderem
- ☒ Ręczny system zamykania (ograniczone zastosowanie dla kluczowych pracowników, do wykorzystania w przypadku awarii systemów kontroli dostępu)
- ☒ CCTV w punktach wejścia (biuro i centra danych)
- ☒ Zamki bezpieczeństwa
- ☒ Zarządzanie gośćmi w recepcji
- ☒ Staranny dobór personelu sprzątającego
- ☒ Obowiązek widocznego noszenia identyfikatorów dostępu
- ☒ Wdrożono odrębną, określoną i udokumentowaną kontrolę dostępu do centrów danych i serwerowni dla osób upoważnionych. Dostęp osób upoważnionych jest udokumentowany nazwiskiem i numerem karty lub tokena. Dla centrów danych wdrożone są odrębne systemy kontroli dostępu

(ii) Kontrola dostępu (systemy)

Zapobieganie nieuprawnionemu użyciu systemów przetwarzania danych

- ☒ Przypisywanie uprawnień użytkowników
- ☒ Przypisywanie haseł
- ☒ Uwierzytelnianie za pomocą nazwy użytkownika / hasła
- ☒ Stosowanie systemów zapobiegania włamaniom
- ☒ Stosowanie sprzętowych zapór sieciowych
- ☒ Tworzenie profili użytkowników
- ☒ Środki dodatkowe: zapory sieciowe aplikacji internetowych, regularne skanowanie podatności, regularne testy penetracyjne, zarządzanie poprawkami, minimalne wymagania dotyczące złożoności haseł i wymuszania ich zmiany, stosowanie skanerów antywirusowych
- ☒ Przypisywanie profili użytkowników do systemów IT
- ☒ Wykorzystanie technologii VPN
- ☒ Szyfrowanie przenośnych nośników danych
- ☒ Zastosowanie centralnej administracji smartfonem (na przykład: zdalne czyszczenie smartfonu)
- ☒ Szyfrowanie dysków w laptopach / notebookach
- ☒ Zastosowanie zapory programowej (klienci biurowi)

(iii) Kontrola dostępu (dane)

Gwarancja że upoważnieni użytkownicy systemu przetwarzania danych mogą mieć dostęp wyłącznie do danych, do których zostali upoważnieni, oraz (ii) zapobieganie odczytywaniu danych osobowych w czasie, gdy są one używane, w ruchu lub w stanie spoczynku, bez upoważnienia.

- ☒ Tworzenie koncepcji autoryzacji
- ☒ Liczba administratorów zredukowana do „absolutnej konieczności”
- ☒ Rejestrowanie dostępu do aplikacji, zwłaszcza podczas wprowadzania, modyfikacji i usuwania danych
- ☒ Bezpieczna sanityzacja nośników przed ponownym użyciem
- ☒ Korzystanie z niszczarek lub usług (jeśli to możliwe, z zabezpieczeniem prywatności)
- ☒ Szyfrowanie dysków (taśmy z kopiami zapasowymi do przechowywania poza siedzibą firmy, laptopy)
- ☒ Zarządzanie uprawnieniami przez administratorów systemu
- ☒ Polityka haseł, w tym długość haseł, zarządzanie zmianami haseł
- ☒ Bezpieczne przechowywanie nośników danych
- ☒ Rejestrowanie bezpiecznego niszczenia nośników danych
- ☒ Zgodne z przepisami niszczenie nośników danych (DIN 66399)

(iv) Segregowane przetwarzanie

Zapewnienie, że dane, które są gromadzone w różnych celach, mogą być przetwarzane oddzielnie:

- ☒ Utworzenie koncepcji zezwolenia
- ☒ Udostępnianie rekordów z atrybutami celu / polami danych
- ☒ Logiczne rozdzielenie klientów (w oprogramowaniu)
- ☒ W przypadku danych pseudonimowych: wydzielenie pliku odwzorowującego i przechowywanie w

	☒ Zatwierdzone i udokumentowane prawa do baz danych	oddzielnym zabezpieczonym systemie informatycznym ☒ Rozdzielenie systemów produkcyjnych i testowych

•

Integralność

Art. 32 (1) (b) RODO

(i) Kontrola transferu

Zapewnienie, że dane osobowe nie mogą być odczytane, skopiowane lub zmodyfikowane podczas transmisji elektronicznej lub podczas transportu lub przechowywania na dysku. Dodatkowo kontrola i ustalanie, do jakich organów dopuszczalne jest przekazywanie danych osobowych dostarczanych przez urządzenia teleinformatyczne:

☒ Tworzenie specjalnych linii lub tuneli VPN	☒ Ujawnianie danych w formie anonimowej lub pseudonimowej
☒ Dokumentacja dotycząca odbiorców danych oraz okresów ich dostarczania, w tym uzgodnionych terminów usuwania danych	☒ Tworzenie przeglądu operacji regularnego składania wniosków i dostaw
☒ Podczas transportu fizycznego staranny dobór personelu i pojazdów transportowych (składowanie taśm poza miejscem zamieszkania)	☒ Podczas transportu fizycznego zabezpieczenie pojemników transportowych/opakowania (taśma poza miejscem składowania)
☒ Szyfrowanie dysków (taśmy zapasowe do przechowywania poza siedzibą firmy)	☒ Szyfrowanie TLS całej komunikacji (Web-Client, API, aplikacje mobilne)

(ii) Sterowanie wejściem

Zapewnienie, późniejsza kontrola i ustalenie, czy i przez kogo dane osobowe zostały wprowadzone, zmienione lub usunięte w systemach przetwarzania danych:

☒ Rejestrowanie wprowadzania, modyfikacji i usuwania danych	☒ Stworzenie przeglądu, które aplikacje mają prawo do wprowadzania, modyfikowania lub usuwania jakich danych
Możliwość śledzenia wprowadzania, modyfikowania i usuwania danych przez poszczególne nazwy użytkowników (nie grupy użytkowników)	☒ Przechowywanie formularzy, za pomocą których dane zostały pozyskane podczas zautomatyzowanego przetwarzania
☒ Przyznawanie praw do wprowadzania, zmiany lub usuwania danych na podstawie koncepcji autoryzacji	

Dostępność i odporność

Art. 32 (1) (b) RODO

(i) Kontrola dostępności

Zapewnienie ochrony danych osobowych przed przypadkowym zniszczeniem lub utratą:

☒ Zasilacze bezprzerwowe (UPS)	☒ Klimatyzacja w serwerowniach
☒ Urządzenia do monitorowania temperatury i wilgotności w serwerowniach	☒ Listwy ochronne w serwerowniach
☒ Systemy wykrywania ognia i dymu	☒ Gaśnice w serwerowniach
☒ Alarm w przypadku wykrycia nieuprawnionego wejścia do serwerowni	☒ Tworzenie koncepcji backupu i odzyskiwania danych
☒ Testowanie odzyskiwania danych	☒ Przygotowanie planu działania w sytuacjach awaryjnych
☒ Bezpieczne przechowywanie kopii zapasowych danych poza siedzibą firmy	☒ Serwerownie niezlokalizowane pod instalacjami sanitarnymi
☒ Na terenach zalewowych: serwerownie powyżej granicy wody	☒ Dwa centra danych w Niemczech w konfiguracji aktywny-aktywny w celu wsparcia odporności.

Proces regularnego przeglądu, analizy i oceny

Art.32 (1) (d);

Art.25 (1) RODO

(i) Kontrola zamówień

Zapewnienie, że dane osobowe, które są przetwarzane w imieniu Administratora, będą przetwarzane wyłącznie zgodnie z jego poleceniami:

☒ Wybór wykonawcy poprzez przegląd historii (w szczególności bezpieczeństwo danych)	☒ Wcześniejsze sprawdzenie dokumentacji i środków bezpieczeństwa podjętych przez wykonawcę
☒ Pisemne instrukcje dla wykonawcy (na przykład przez DPA) (RODO)	☒ Zobowiązanie pracowników wykonawcy do zachowania poufności danych (RODO)
☒ W wymaganym zakresie: zapewnienie, że wykonawcy wyznaczyli Inspektorów Ochrony Danych	☒ Zapewnienie bezpiecznego niszczenia danych po zakończeniu umowy
☒ Uzgodniono skuteczne prawa kontroli nad podmiotami przetwarzającymi dane	☒ Stały przegląd wykonawców i ich działań
☒ Zarządzanie ochroną danych (ISMS)	☒ Zarządzanie reagowaniem na incydenty
	☒ Ochrona danych w fazie projektowania oraz domyślna (Art.25 (2) RODO)

ZAŁĄCZNIK IV / Przepisy dodatkowe

Kontroler i Przetwarzający zgadzają się na uzupełnienie Klauzul o następujące postanowienia:

(a) Jeżeli którekolwiek z postanowień niniejszych klauzul będzie w dowolnym momencie nieważne lub niewykonalne na mocy obecnego lub przyszłego prawa, orzecznictwa lub wytycznych i decyzji wykonawczych właściwego organu nadzoru, będzie ono nieskuteczne w zakresie, ale tylko w zakresie takiej nieważności lub niewykonalności bez unieważnienia pozostałych części niniejszej klauzuli, a takie pozostałe części niniejszych klauzul będą nadal w pełni obowiązywać. W przypadku, gdy którekolwiek z postanowień niniejszych klauzul zostanie uznane za nieważne lub niewykonalne, strony będą prowadzić w dobrej wierze negocjacje w celu zastąpienia takiego postanowienia innym postanowieniem, które będzie ważne lub wykonalne i które będzie możliwie najbliższe postanowieniom uznanym za nieważne lub niewykonalne.

(b) Wszelkie zmiany niniejszych klauzul wymagają formy pisemnej pod rygorem nieważności, o ile nie postanowiono inaczej.

(c) Wszystkie postanowienia Klauzul dotyczące prawa do wypowiedzenia stosuje się również bezpośrednio do umowy będącej podstawą współpracy (np. umowy o świadczenie usług, na podstawie której Przetwarzający świadczy usługi, z którymi wiąże się przetwarzanie danych osobowych).

(d) Niniejsze klauzule podlegają prawu holenderskiemu.

ZAŁĄCZNIK V / Lista podwykonawców przetwarzania Webfleet

Administrator zezwolił w drodze Ogólnego Upoważnienia na korzystanie z następujących podwykonawców przetwarzania:

Firma	Lokalizacja	Usługi
Bayerische Motoren Werke Aktiengesellschaft (BMW)	Petuelring 130, 80788 Monachium, Niemcy	Udostępnienie danych API dotyczących ich pojazdów BMW Group (BMW, MINI) firmie Bridgestone Mobility Solutions B.V. i jej podmiotom stowarzyszonym, w celu umożliwienia świadczenia Usługi WEBFLEET jej klientom.
DAKO Systemtechnik und Service GmbH & Co. KG	Brusseler Str. 7-11, 07747 Jena, Niemcy	Manager Tachografu WEBFLEET
Ford Smart Mobility U.K. Limited	Business Unit 2, Broadcast Centre, Here East, Queen Elizabeth Olympic Park, Stratford, London, Anglia, E20 3BS	Udostępnienie danych API dotyczących pojazdów marki Ford firmie Bridgestone Mobility Solutions B.V. i jej podmiotom stowarzyszonym, w celu umożliwienia świadczenia Usługi WEBFLEET jej klientom.
Google Dublin, Google Ireland Ltd.	Gordon House Barrow St. Dublin 4, Irlandia	Google Maps API: https://business.safety.google/controllerterms/
Lytx, INC.	170 Midsummer Blvd, Milton Keynes MK9 1BP, Wielka Brytania; oraz HaMada Street 7, Yokne'am Illit, Izrael	Usługi związane z kamerą (sprzęt i oprogramowanie), w tym obsługa klienta Lytx używa następujących podwykonawców przetwarzania: • Amazon Web Services EMEA SRL (Hosting) | 38 Avenue John F. Kennedy, L-1855, Luksemburg • Logz.io UK Limited (monitorowanie danych) | 37 Broadhurst Gardens, Londyn, Wielka Brytania, NW6 3QT
TomTom International B.V.	De Ruijterkade 154 1011 AC Amsterdam Holandia	Dla klientów, którzy wykupili usługę WEBFLEET, te usługi zlecone przez Podmiot przetwarzający będą świadczone przez TomTom International jako partnera strategicznego. Usługi obejmują ruch drogowy, kamery bezpieczeństwa, wyszukiwanie lokalne, usługi dotyczące stanu dróg, informacje pogodowe i ceny paliw.
Webfleet Solutions Development Germany GmbH	Inselstrasse 22, 04103 Leipzig, Niemcy	Bezpieczny hub technologiczny z certyfikatem ISO 27001:2017, obejmujący Technologie Informatyczne, Bezpieczny Rozwój Oprogramowania oraz kolokowane centra danych w połączeniu z Platformą Usług Telematycznych WEBFLEET dostarczaną do Bridgestone Mobility Solutions B.V.