
title: Umowa powierzenia przetwarzania danych osobowych (DPA) — TourFlow status: PROJEKT (mocny zarys) — do przeglądu przez radcę prawnego / IOD przed podpisaniem

wersja: 0.1 (standardowa umowa powierzenia wg art. 28 RODO)

UWAGA REDAKCYJNA — usunąć przed podpisaniem. Standardowa umowa powierzenia (art. 28 RODO), spójna z docs/regulamin.md i docs/polityka-prywatnosci.md. **Role:** Organizator (biuro podróży) = **Administrator** danych Klientów końcowych; WhiteIT (TourFlow) = **Podmiot przetwarzający**. Podprocesory uzupełnieni: OVH (UE), Mistral AI (UE), Google/Gmail (USA, DPF/SCC). **Pozostaje przy podpisywaniu:** dane konkretnego Organizatora (strony umowy) — wpisywane per klient. Przed podpisaniem: przegląd prawnika / IOD. Forma: dokument może być zawierany elektronicznie jako załącznik do Umowy (zgodnie z procesem z Regulaminu § 6).

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta pomiędzy:

Administratorem — **[[NAZWA / IMIĘ I NAZWISKO ORGANIZATORA]]**, **[[ADRES]]**, NIP **[[NIP]]**, **[[REGON / KRS, jeśli dotyczy]]** (dalej: **Administrator**),

a

Podmiotem przetwarzającym — **WhiteIT** — Michał Basiński prowadzący działalność gospodarczą pod firmą Michał Basiński WhiteIT, ul. Łąkowa 1, 62-220 Niechanowo, NIP 7842500273, REGON 364808970, wpisany do CEIDG (dalej: **Podmiot przetwarzający**),

zwanymi dalej łącznie **Stronami**, a każda z osobna **Stroną**.

§ 1. Definicje i postanowienia ogólne

- Pojęcia: **RODO**, **dane osobowe**, **przetwarzanie**, **administrator**, **podmiot przetwarzający**, **naruszenie ochrony danych osobowych**, **odbiorca** — mają znaczenie nadane im w RODO (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.).
- Pojęcia: **Aplikacja / TourFlow**, **Organizator**, **Użytkownik**, **Klient końcowy**, **Umowa**, **Regulamin** — mają znaczenie nadane im w Regulaminie świadczenia usług drogą elektroniczną TourFlow.
- Niniejsza umowa (dalej: **Umowa powierzenia**) określa zasady przetwarzania przez Podmiot przetwarzający danych osobowych powierzonych przez Administratora w związku z korzystaniem z Aplikacji na podstawie Umowy.

4. Umowa powierzenia stanowi integralną część Umowy. W razie sprzeczności w zakresie przetwarzania danych osobowych pierwszeństwo mają postanowienia Umowy powierzenia.

§ 2. Przedmiot, charakter, cel i czas powierzenia

1. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych w zakresie i w celu niezbędnym do świadczenia usług określonych w Umowie i Regulaminie, tj. udostępniania i obsługi Aplikacji w modelu usługi.
2. **Charakter i cel przetwarzania:** przetwarzanie danych osobowych w imieniu Administratora wyłącznie w celu technicznego umożliwienia Administratorowi korzystania z funkcjonalności Aplikacji (m.in. obsługa wycieczek, uczestników, umów, dokumentów, rozliczeń, komunikacji e-mail oraz przygotowania danych na potrzeby obowiązków sprawozdawczych Administratora), zgodnie z dokumentacją Aplikacji i poleceniami Administratora.
3. **Kategorie osób, których dane dotyczą, oraz rodzaje danych osobowych** określa **Załącznik nr 1**.
4. **Czas trwania przetwarzania:** powierzenie obowiązuje przez czas obowiązywania Umowy. Po jej zakończeniu stosuje się § 11 (zwrot lub usunięcie danych).
5. Podmiot przetwarzający nie nabywa żadnych praw do powierzonych danych osobowych i nie może wykorzystywać ich do własnych celów.

§ 3. Polecenia Administratora

1. Podmiot przetwarzający przetwarza powierzone dane osobowe wyłącznie na udokumentowane polecenie Administratora, chyba że obowiązek przetwarzania nakłada na niego prawo Unii Europejskiej lub prawo polskie; w takim przypadku Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym przed przetwarzaniem, o ile prawo to nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny.
2. Za udokumentowane polecenia uznaje się polecenia wynikające z Umowy, Regulaminu, niniejszej Umowy powierzenia oraz czynności wykonywane przez Administratora i Użytkowników w Aplikacji (konfiguracja, wprowadzanie i przetwarzanie danych, korzystanie z funkcjonalności). Dodatkowe polecenia mogą być przekazywane drogą elektroniczną na adresy kontaktowe Stron.
3. Podmiot przetwarzający niezwłocznie informuje Administratora, jeżeli jego zdaniem polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych osobowych.

§ 4. Obowiązki Podmiotu przetwarzającego

Podmiot przetwarzający zobowiązuje się w szczególności do:

1. przetwarzania danych wyłącznie zgodnie z § 3 oraz z RODO;
2. zapewnienia, by osoby upoważnione do przetwarzania powierzonych danych zobowiązały się do zachowania poufności lub podlegały odpowiedniemu ustawowemu

obowiązkowi zachowania tajemnicy, oraz nadawania upoważnień do przetwarzania danych w niezbędnym zakresie;

3. wdrożenia i utrzymywania środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania, odpowiednich do ryzyka, zgodnie z art. 32 RODO — opisanych w **Załączniku nr 2**;
4. przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego (podpowierzenia), o których mowa w § 5;
5. pomocy Administratorowi — w miarę możliwości i poprzez odpowiednie środki techniczne i organizacyjne — w wywiązaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw (rozdział III RODO);
6. pomocy Administratorowi w wywiązaniu się z obowiązków określonych w art. 32–36 RODO (bezpieczeństwo przetwarzania, zgłaszanie i zawiadamianie o naruszeniach, ocena skutków dla ochrony danych oraz uprzednie konsultacje), z uwzględnieniem charakteru przetwarzania oraz informacji dostępnych Podmiotowi przetwarzającemu;
7. po zakończeniu świadczenia usług — zwrotu lub usunięcia danych zgodnie z § 11;
8. udostępniania Administratorowi informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwienia audytów, w tym inspekcji, zgodnie z § 8.

§ 5. Podpowierzenie (dalsze podmioty przetwarzające)

1. Administrator udziela Podmiotowi przetwarzającemu **ogólnej zgody** na korzystanie z usług dalszych podmiotów przetwarzających (podprocesorów) w celu świadczenia usług, w szczególności dostawców infrastruktury, hostingu, poczty elektronicznej oraz narzędzi wspomagających przetwarzanie dokumentów (w tym narzędzi opartych na sztucznej inteligencji). Aktualną listę podprocesorów zawiera **Załącznik nr 3**.
2. Podmiot przetwarzający informuje Administratora o zamierzonych zmianach dotyczących dodania lub zastąpienia podprocesorów, dając Administratorowi możliwość wyrażenia sprzeciwu. Informacja może być przekazana drogą elektroniczną lub przez udostępnienie zaktualizowanej listy w Aplikacji lub na stronie internetowej, z co najmniej **14-dniowym** wyprzedzeniem.
3. Jeżeli Administrator wniesie uzasadniony sprzeciw wobec zmiany w terminie **14 dni**, a Strony nie uzgodnią rozwiązania, Administrator może wypowiedzieć Umowę w części dotyczącej usług wymagających spornego podprocesora, na zasadach określonych w Umowie.
4. Podmiot przetwarzający nakłada na każdego podprocesora — w drodze umowy — obowiązki w zakresie ochrony danych odpowiadające obowiązkom z niniejszej Umowy powierzenia, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych (art. 28 ust. 4 RODO). Podmiot przetwarzający odpowiada wobec Administratora za działania i zaniechania podprocesorów jak za własne.

§ 6. Prawa osób, których dane dotyczą

1. Podmiot przetwarzający, uwzględniając charakter przetwarzania, pomaga Administratorowi — poprzez odpowiednie środki techniczne i organizacyjne (w tym

funkcjonalności Aplikacji umożliwiające dostęp, sprostowanie, usunięcie lub eksport danych) — w wywiązaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą.

2. Jeżeli osoba, której dane dotyczą, zwróci się bezpośrednio do Podmiotu przetwarzającego z żądaniem dotyczącym danych powierzonych, Podmiot przetwarzający niezwłocznie przekazuje takie żądanie Administratorowi i nie realizuje go samodzielnie, chyba że działa na polecenie Administratora lub obowiązek wynika z przepisów prawa.

§ 7. Naruszenia ochrony danych osobowych

1. Podmiot przetwarzający, po stwierdzeniu naruszenia ochrony powierzonych danych osobowych, zgłasza je Administratorowi **bez zbędnej zwłoki**, nie później niż w ciągu **48 godzin** od stwierdzenia naruszenia.
2. Zgłoszenie zawiera co najmniej, w miarę dostępności: opis charakteru naruszenia (w tym kategorie i przybliżoną liczbę osób oraz wpisów, których dotyczy), prawdopodobne konsekwencje, opis zastosowanych lub proponowanych środków zaradczych oraz dane kontaktowe punktu, w którym można uzyskać informacje.
3. Podmiot przetwarzający współdziała z Administratorem przy wyjaśnianiu okoliczności naruszenia oraz przy realizacji obowiązków Administratora wobec organu nadzorczego i osób, których dane dotyczą. Zgłaszanie naruszeń organowi nadzorczemu oraz zawiadamianie osób, których dane dotyczą, należy do Administratora.

§ 8. Audyt i informacje

1. Podmiot przetwarzający udostępnia Administratorowi informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwia Administratorowi (lub upoważnionemu przez niego audytorowi) przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.
2. Audyt odbywa się po uprzednim powiadomieniu z rozsądnym wyprzedzeniem (co najmniej **14 dni**), w godzinach pracy, w sposób niezakłócający działalności Podmiotu przetwarzającego oraz z poszanowaniem poufności i ochrony danych innych klientów. Strony mogą uzgodnić, że potwierdzenie zgodności następuje w pierwszej kolejności przez udostępnienie informacji, dokumentacji środków bezpieczeństwa lub raportów/certyfikatów.
3. Osoby przeprowadzające audyt zobowiązane są do zachowania poufności. Zasady ponoszenia kosztów audytu mogą określać Umowa lub odrębne uzgodnienia Stron.

§ 9. Przekazywanie danych poza Europejski Obszar Gospodarczy (EOG)

1. Podmiot przetwarzający co do zasady przetwarza powierzone dane na terytorium Polski lub EOG.
2. Przekazanie powierzonych danych do państwa trzeciego (poza EOG) lub organizacji międzynarodowej może nastąpić wyłącznie wówczas, gdy zapewniono podstawę i zabezpieczenia wymagane RODO, w szczególności decyzję Komisji Europejskiej o

odpowiednim stopniu ochrony, standardowe klauzule umowne (SCC) albo inną podstawę przewidzianą w rozdziale V RODO, wraz z dodatkowymi środkami zabezpieczającymi, jeżeli są wymagane.

3. Hosting oraz funkcje oparte na sztucznej inteligencji realizowane są w EOG (OVH oraz Mistral AI w UE). Przekazanie poza EOG może wystąpić w związku z usługą poczty elektronicznej (Google) — na podstawie programu EU-US Data Privacy Framework lub standardowych klauzul umownych (SCC). Wykaz podprocesorów wraz z lokalizacją i podstawą transferu zawiera **Załącznik nr 3**.

§ 10. Odpowiedzialność

1. Każda ze Stron odpowiada za szkody spowodowane przetwarzaniem niezgodnym z RODO na zasadach określonych w art. 82 RODO oraz w przepisach prawa.
2. W zakresie wzajemnych rozliczeń Stron (regres) zastosowanie mają ograniczenia odpowiedzialności określone w Umowie i Regulaminie, w zakresie dopuszczalnym przepisami prawa. Ograniczenia te nie wpływają na odpowiedzialność Stron wobec osób, których dane dotyczą, ani na odpowiedzialność, której nie można wyłączyć lub ograniczyć na podstawie bezwzględnie obowiązujących przepisów.
3. Administrator odpowiada za zgodność z prawem powierzenia oraz za posiadanie właściwej podstawy prawnej przetwarzania danych, które wprowadza lub przekazuje do Aplikacji, a także za wykonanie wobec osób, których dane dotyczą, obowiązków informacyjnych.

§ 11. Zwrot lub usunięcie danych po zakończeniu

1. Po zakończeniu świadczenia usług związanych z przetwarzaniem Podmiot przetwarzający — zależnie od decyzji Administratora — usuwa lub zwraca Administratorowi powierzone dane osobowe oraz usuwa ich istniejące kopie, chyba że prawo Unii lub prawo polskie nakazują przechowywanie danych osobowych.
2. Administrator może pobrać (wyeksportować) powierzone dane w okresie **30 dni** od zakończenia Umowy (zgodnie z Regulaminem § 19). Po upływie tego okresu Podmiot przetwarzający może usunąć dane, z zastrzeżeniem ust. 1.
3. Na żądanie Administratora Podmiot przetwarzający potwierdza usunięcie danych.

§ 12. Czas obowiązywania i postanowienia końcowe

1. Umowa powierzenia obowiązuje przez czas obowiązywania Umowy i wygasa wraz z nią, z zachowaniem § 11.
2. W sprawach nieuregulowanych stosuje się RODO, przepisy prawa polskiego oraz postanowienia Umowy i Regulaminu.
3. Zmiany Umowy powierzenia wymagają formy uzgodnionej dla zmian Umowy. Aktualizacja Załącznika nr 3 (lista podprocesorów) następuje w trybie § 5.
4. Załączniki stanowią integralną część Umowy powierzenia:
 - **Załącznik nr 1** — kategorie osób i rodzaje danych;
 - **Załącznik nr 2** — środki techniczne i organizacyjne;
 - **Załącznik nr 3** — lista podprocesorów.

Załącznik nr 1 — Kategorie osób i rodzaje powierzonych danych

Przedmiot przetwarzania: dane wprowadzane do Aplikacji przez Administratora i Użytkowników w związku z obsługą działalności organizatora turystyki (wycieczki grupowe).

Kategorie osób, których dane dotyczą (w zakresie wprowadzonym przez Administratora): - Klienci końcowi i uczestnicy wycieczek/impres oraz ich opiekunowie; - osoby kontaktowe grup (m.in. szkoły, parafie, firmy, stowarzyszenia); - kadra przypisana do wycieczek (piloci, przewodnicy) — w zakresie danych wprowadzanych przez Administratora; - inne osoby, których dane Administrator wprowadza do Aplikacji w związku z umowami, dokumentami lub rozliczeniami.

Rodzaje danych osobowych (w zakresie wprowadzonym przez Administratora): - dane identyfikacyjne i kontaktowe (imię, nazwisko, telefon, e-mail, adres); - dane dotyczące uczestnictwa i umów (wycieczka, numer i dane umowy, liczba osób, dopłaty); - dane rozliczeniowe (wpłaty, zwroty, należności) oraz dane do dokumentów (faktury, listy, vouchery, karta pilota); - data urodzenia, numer PESEL oraz dane dokumentu podróży (np. paszport) — wprowadzane przez Administratora na potrzeby umów, ubezpieczeń lub wyjazdów zagranicznych; - inne dane podane w treści dokumentów lub uwag wprowadzonych przez Administratora.

Dane szczególnych kategorii (art. 9 RODO). Aplikacja nie jest przeznaczona do przetwarzania danych szczególnych kategorii (np. o stanie zdrowia czy diecie uczestnika). Administrator zobowiązany jest unikać wprowadzania takich danych; jeżeli ich przetwarzanie jest wyjątkowo niezbędne, Administrator zapewnia właściwą podstawę z art. 9 RODO, a Strony uzgadniają dodatkowe zabezpieczenia.

Załącznik nr 2 — Środki techniczne i organizacyjne (art. 32 RODO)

Podmiot przetwarzający stosuje w szczególności: - kontrolę dostępu i uwierzytelnianie Użytkowników (logowanie, hasła przechowywane w postaci skrótów, zarządzanie sesją), nadawanie dostępu według ról i zakresu uprawnień; - rozdzielenie danych poszczególnych Administratorów (izolacja danych w ramach Aplikacji); - szyfrowanie połączeń (transmisji danych); - rejestrowanie zdarzeń i aktywności (logi, dziennik aktywności) na potrzeby bezpieczeństwa i rozliczalności; - wykonywanie kopii zapasowych oraz procedury przywracania danych; - procedury reagowania na naruszenia ochrony danych; - zobowiązanie osób upoważnionych do zachowania poufności; - okresowy przegląd i aktualizację stosowanych zabezpieczeń odpowiednio do ryzyka.

[[DO UZUPEŁNIENIA: doprecyzować zgodnie z faktycznie wdrożonymi środkami (np. szczegóły szyfrowania w spoczynku, polityka haseł, retencja kopii, lokalizacja serwerów, zarządzanie podatnościami).]]

Załącznik nr 3 — Lista podprocesorów

Podprocesor	Rola / zakres	Lokalizacja przetwarzania	Transfer poza EOG / zabezpieczenia
OVH (OVHcloud)	hosting i infrastruktura Aplikacji	EOG (UE)	nie dotyczy
Mistral AI (Mistral AI SAS, [15 rue des Halles, 75001 Paryż, Francja]) — API modeli językowych	wspomaganie odczytu i przetwarzania dokumentów oraz planowania wycieczek (funkcje AI); wyłącznie po aktywacji funkcji AI dla Konta; dane nie są wykorzystywane przez dostawcę do trenowania modeli na warunkach API	EOG (UE)	nie dotyczy
Google (Gmail / Google Workspace)	wysyłka wiadomości e-mail	Google (USA)	poza EOG — EU-US Data Privacy Framework / SCC

Narzędzie do generowania dokumentów PDF oraz pobieranie kursów walut (NBP) — jeżeli realizowane są w ramach infrastruktury Podmiotu przetwarzającego i bez udziału zewnętrznego procesora danych osobowych — nie stanowią odrębnego podpowierzenia. **[[Zweryfikować przy wdrożeniu.]]**