

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Wersja: 2026-10-01 (v1.0) · zastępuje wersję 0.1 · integralna część Umowy o korzystanie z TourFlow

zawarta pomiędzy:

Administratorem — Organizatorem korzystającym z Aplikacji TourFlow: w trybie indywidualnym **[[NAZWA / IMIĘ I NAZWISKO ORGANIZATORA]]**, **[[ADRES]]**, NIP **[[NIP]]**, **[[REGON / KRS]]**; w Samodzielnej rejestracji — podmiotem, którego dane wskazano w formularzu rejestracji i w danych Konta (dalej: **Administrator**),

a

Podmiotem przetwarzającym — **WhiteIT** — Michał Basiński prowadzący działalność gospodarczą pod firmą Michał Basiński WhiteIT, ul. Łakowa 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, postanowienia ogólne i sposób zawarcia

- 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**, **Panel**, **Organizator**, **Użytkownik**, **Pilot**, **Klient końcowy**, **Konto**, **Właściciel Konta**, **Umowa**, **Warunki Indywidualne**, **Samodzielna rejestracja**, **Okres Testowy**, **Plan**, **Regulamin** — mają znaczenie nadane im w Regulaminie świadczenia usług drogą elektroniczną TourFlow (dalej: **Regulamin**).
- 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. Jest umową, o której mowa w art. 28 ust. 3 RODO.
- Umowa powierzenia stanowi integralną część Umowy. W razie sprzeczności w zakresie przetwarzania danych osobowych pierwszeństwo mają postanowienia Umowy powierzenia.
- Sposób zawarcia**. W trybie indywidualnym Umowa powierzenia jest zawierana wraz z Umową w sposób opisany w § 6 ust. 2 Regulaminu. W Samodzielnej rejestracji Umowa powierzenia zostaje zawarta z chwilą zaakceptowania jej treści łącznie z Regulaminem przez zaznaczenie odpowiedniego pola w formularzu rejestracji Konta; osoba akceptująca oświadcza, że jest umocowana do zawarcia Umowy powierzenia w imieniu Administratora. Podmiot przetwarzający rejestruje datę, wersję dokumentu, adres IP i identyfikator przeglądarki osoby akceptującej; zapis ten stanowi dowód zawarcia Umowy powierzenia w formie elektronicznej.

§ 2. Przedmiot, charakter, cel i czas powierzenia

- 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.
- Cel przetwarzania**: techniczne umożliwienie Administratorowi korzystania z funkcjonalności Aplikacji (obsługa wycieczek, uczestników, umów, zapisów online, dokumentów, rozliczeń, komunikacji e-mail, portalu pilota oraz przygotowanie danych na potrzeby obowiązków sprawozdawczych Administratora), zgodnie z dokumentacją Aplikacji i poleceniami Administratora.

3. **Charakter przetwarzania:** przetwarzanie w systemie informatycznym udostępnianym zdalnie, obejmujące w szczególności przechowywanie, porządkowanie, udostępnianie Administratorowi, jego Użytkownikom i Pilotom, wykonywanie kopii zapasowych, generowanie dokumentów i zestawień na polecenie Administratora, wysyłkę wiadomości e-mail zleconych przez Administratora, przekazywanie wykazów do Ubezpieczeniowego Funduszu Gwarancyjnego na polecenie Administratora (jeżeli funkcja jest aktywna), przetwarzanie treści dokumentów przez funkcje AI na polecenie Administratora (jeżeli funkcja jest aktywna) oraz usuwanie danych.
4. **Kategorie osób, których dane dotyczą, oraz rodzaje danych osobowych** określa **Załącznik nr 1**.
5. **Czas trwania przetwarzania:** powierzenie obowiązuje przez czas obowiązywania Umowy, w tym w Okresie Testowym oraz w okresie tylko do odczytu po zakończeniu Umowy, aż do usunięcia danych zgodnie z § 11.
6. Podmiot przetwarzający nie ma dostępu do treści powierzonych danych w toku zwykłego świadczenia usług. Dostęp personelu Podmiotu przetwarzającego — przez konto serwisowe opisane w Regulaminie § 7 ust. 5 albo bezpośrednio do bazy danych — następuje wyłącznie w celu diagnostyki błędów, wsparcia technicznego na zgłoszenie Administratora, zapewnienia bezpieczeństwa lub wykonania obowiązków prawnych i jest rejestrowany.
7. Podmiot przetwarzający nie nabywa żadnych praw do powierzonych danych osobowych, nie może wykorzystywać ich do własnych celów, w szczególności marketingowych, ani do trenowania modeli sztucznej inteligencji.

§ 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, Użytkowników i Pilotów w Aplikacji (konfiguracja, wprowadzanie i przetwarzanie danych, korzystanie z funkcjonalności, w tym włączenie dodatkowych pól danych uczestników, funkcji AI, zapisów online, wysyłki do UFG). 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, ochrony formularzy, obsługi płatności i fakturowania za Usługę oraz modeli językowych wykorzystywanych przez funkcje AI. Aktualną listę podprocesorów zawiera **Załącznik nr 3**; podprocesorzy oznaczeni jako opcjonalni przetwarzają dane wyłącznie po aktywacji danej funkcji przez Administratora.
2. Podmiot przetwarzający informuje Administratora o zamierzonych zmianach dotyczących dodania lub zastąpienia podprocesorów, dając Administratorowi możliwość wyrażenia sprzeciwu. Informacja jest przekazywana drogą elektroniczną na adres Właściciela Konta lub osoby wskazanej w Umowie oraz przez udostępnienie zaktualizowanego Załącznika nr 3 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, a gdy nie jest to możliwe — Umowę w całości, na zasadach określonych w Umowie i Regulaminie.
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 (w szczególności uczestnik lub osoba zapisująca się przez formularz zapisów online), 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, na adres e-mail Właściciela Konta lub osoby wskazanej w Umowie.
2. Zgłoszenie zawiera co najmniej, w miarę dostępności: opis charakteru naruszenia (w tym kategorii 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**), nie częściej niż raz w roku (poza przypadkiem naruszenia lub żądania organu), w Dni Robocze, w sposób niezakłócający działalności Podmiotu przetwarzającego oraz z poszanowaniem poufności i ochrony danych innych Administratorów. Potwierdzenie zgodności następuje w pierwszej kolejności przez udostępnienie informacji, dokumentacji środków bezpieczeństwa (Załącznik nr 2) lub raportów.
3. Osoby przeprowadzające audyt zobowiązane są do zachowania poufności. Koszty audytu ponosi Administrator, chyba że audyt wykaże istotne naruszenie Umowy powierzenia przez Podmiot przetwarzający albo Umowa stanowi inaczej.

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

1. Podmiot przetwarzający co do zasady przetwarza powierzone dane na terytorium 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 i kopie zapasowe realizowane są w EOG (OVH: Polska i Niemcy), a funkcje oparte na sztucznej inteligencji — w EOG (Mistral AI, UE). Przekazanie poza EOG może wystąpić w związku z usługą poczty elektronicznej (Google) oraz ochroną formularzy (Cloudflare) — 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 (także danych zbieranych przez publikowane przez niego formularze zapisów online), za minimalizację zakresu danych, w tym za decyzję o włączeniu dodatkowych pól danych uczestników, 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. **Podstawową formą zwrotu danych** jest samodzielne pobranie ich przez Administratora z Aplikacji (zestawienia XLSX/CSV, wygenerowane dokumenty PDF, przesłane pliki) w okresie **30 dni** od zakończenia Umowy albo Okresu Testowego bez aktywacji płatnego Planu, gdy Konto pozostaje dostępne w trybie tylko do odczytu (Regulamin § 19). Na wniosek Administratora złożony w tym okresie Podmiot przetwarzający przygotowuje eksport zbiorczy w terminie 14 dni.

3. **Konta z Samodzielnej rejestracji:** po upływie 30 dni dostęp zostaje zablokowany, a Podmiot przetwarzający wysyła powiadomienia o zbliżającym się usunięciu na 7 dni i na 1 dzień przed usunięciem; po upływie **60 dni** od zakończenia Umowy albo Okresu Testowego Podmiot przetwarzający trwale usuwa wszystkie powierzone dane z bazy produkcyjnej i magazynu plików.
Umowy w trybie indywidualnym: po upływie 30 dni Podmiot przetwarzający usuwa dane w terminie uzgodnionym z Administratorem, nie później niż w ciągu 60 dni od zakończenia Umowy, chyba że Warunki Indywidualne stanowią inaczej.
4. Dane zawarte w kopiach zapasowych są usuwane przez nadpisanie w cyklu rotacji kopii, nie później niż w ciągu [30] dni od usunięcia z bazy produkcyjnej. Do tego czasu kopie są przechowywane w postaci zaszyfrowanej i nie są wykorzystywane do przetwarzania innego niż odtworzenie po awarii; w razie odtworzenia Podmiot przetwarzający ponownie usuwa dane Administratora.
5. Podmiot przetwarzający zachowuje dane w zakresie, w jakim prawo Unii lub państwa członkowskiego nakazuje ich przechowywanie (w szczególności dokumenty księgowe) oraz zapis dotyczący zawarcia i wykonania Umowy powierzenia (zapis akceptacji, korespondencja) do upływu okresu przedawnienia roszczeń; dane te są w tym okresie przetwarzane wyłącznie w tym celu.
6. Administrator może w każdym czasie w okresie obowiązywania Umowy samodzielnie usuwać wybrane dane w Aplikacji oraz zażądać usunięcia całego Konta przed upływem terminów z ust. 3. Część danych podlega usunięciu miękkimu (oznaczenie jako usunięte, niewidoczne w Aplikacji), a trwałemu — w ramach usunięcia Konta.
7. Na żądanie Administratora złożone po usunięciu Podmiot przetwarzający potwierdza e-mailem 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 następują w trybie przewidzianym dla zmian Regulaminu (Regulamin § 18); aktualizacja Załącznika nr 3 (lista podprocesorów) następuje w trybie § 5; aktualizacja Załącznika nr 2 na korzyść bezpieczeństwa danych nie wymaga zawiadomienia.
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, Użytkowników, Pilotów oraz osoby zapisujące się przez publikowane przez Administratora formularze zapisów online, w związku z obsługą działalności organizatora turystyki (wycieczki grupowe i wyjazdy z zapisami indywidualnymi).

Kategorie osób, których dane dotyczą (w zakresie wprowadzonym przez Administratora lub zebranych przez jego formularze): - Klienci końcowi: uczestnicy wycieczek i imprez, ich opiekunowie, osoby zawierające umowę lub zapisujące uczestników (zamawiający), klienci indywidualni z kartoteki Administratora; - osoby kontaktowe grup (m.in. szkoły, parafie, firmy, stowarzyszenia) oraz przedstawiciele grup; - kadra przypisana do wycieczek (piloci, przewodnicy, kierowcy) — w tym Piloci korzystający z portalu pilota; - pracownicy i współpracownicy Administratora będący Użytkownikami (dane konta: imię, nazwisko, e-mail, telefon); - inne osoby, których dane Administrator wprowadza do Aplikacji w związku z umowami, dokumentami, rozliczeniami lub wydatkami.

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, pakiet, miejsce odbioru, dopłaty, zgody wyrażone przy zapisie online); -

dane rozliczeniowe (wpłaty, zwroty, należności) oraz dane do dokumentów (umowy, listy uczestników, karty wycieczki i pilota, wykazy TFG); - **domyślny zakres danych uczestnika**: imię i nazwisko oraz data urodzenia; **na wniosek Administratora** włączane są dodatkowe pola: numer PESEL, numer i data ważności dokumentu tożsamości (dowód, paszport), miejsce wydania dokumentu, telefon uczestnika, adres i data urodzenia zamawiającego — na potrzeby umów, ubezpieczeń lub wyjazdów zagranicznych; Administrator potwierdza niezbędność tych danych; - dane wydatków i rozliczeń pilota (kwoty, opisy, zdjęcia dokumentów przesłane przez Pilota), jeżeli aktywny jest portal pilota; - treść dokumentów i faktur przesłanych do funkcji AI (dane kontrahentów, kwoty, ewentualne dane osobowe w treści), jeżeli funkcja jest aktywna; - inne dane podane w treści dokumentów, komentarzy 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 w polach opisowych; jeżeli ich przetwarzanie jest wyjątkowo niezbędne, Administrator zapewnia właściwą podstawę z art. 9 RODO.

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

A. Izolacja i kontrola dostępu do danych

1. Każde Konto ma odrębny identyfikator; wszystkie tabele z danymi Administratorów zawierają go jako klucz izolacji.
2. Izolacja wymuszana jest na poziomie silnika bazy danych PostgreSQL (Row Level Security z klauzulą FORCE), niezależnie od kodu aplikacji; aplikacja łączy się z bazą jako użytkownik bez uprawnień do obejścia tej izolacji.
3. Kontekst Konta ustawiany jest w sesji bazy danych na podstawie podpisanego tokenu uwierzytelniającego; brak kontekstu oznacza brak dostępu do danych, nie dostęp do wszystkich danych.
4. Automatyczny test uruchamiany przy każdej zmianie schematu bazy sprawdza, czy każda nowa tabela z danymi Administratorów ma włączoną izolację; wyjątki są wyliczone i uzasadnione w dokumentacji technicznej.
5. Funkcje bazy danych działające z podwyższonymi uprawnieniami (potrzebne np. do logowania przed ustaleniem Konta) są wyliczone, tylko do odczytu, zwracają minimum danych i podlegają przeglądowi przy każdej zmianie.
6. Role w Koncie: użytkownik, właściciel konta (zarządza użytkownikami i konfiguracją), konto serwisowe Podmiotu przetwarzającego (do wsparcia technicznego, niewidoczne na listach, dostęp rejestrowany). Piloci w portalu pilota widzą wyłącznie dane udostępnionych im wycieczek.

B. Uwierzytelnianie i sesje

1. Hasła o długości co najmniej 12 znaków, sprawdzane względem listy haseł powszechnie używanych i danych osobowych użytkownika; przechowywane wyłącznie jako skrót z solą (algorytm klasy bcrypt).
2. Tokeny aktywacji konta, resetu hasła i logowania pilota: losowe, jednorazowe, z ograniczonym czasem ważności, przechowywane w bazie tylko jako skrót SHA-256.
3. Sesje oparte na krótkotrwałych tokenach dostępu i rotowanych tokenach odświeżania w ciasteczkach httpOnly/Secure; wykrycie ponownego użycia zużytego tokenu unieważnia całą rodzinę sesji. Czas sesji 12 godzin, z opcją „zapamiętaj mnie” 7 dni.
4. Ograniczenie liczby prób logowania (limit częstotliwości, czasowa blokada konta po pięciu nieudanych próbach), ochrona CSRF dla uwierzytelnienia opartego na ciasteczkach.
5. Publiczne formularze (rejestracja, reset hasła, zapisy na wycieczki) chronione mechanizmem antybotowym, polem pułapką oraz limitami częstotliwości egzekwowanymi w bazie danych.

C. Szyfrowanie

1. Transmisja: TLS 1.2 lub wyższy na wszystkich połączeniach zewnętrznych (przeglądarka, poczta, API podprocesorów), certyfikaty odnawiane automatycznie.
2. Numer PESEL uczestników szyfrowany w bazie danych kluczem aplikacyjnym przechowywanym poza bazą (konfiguracja wdrożenia).
3. Sekrety integracji (certyfikaty UFG, hasła aplikacyjne, klucze API) przechowywane w postaci zaszyfrowanej lub w konfiguracji wdrożeniowej, nie w kodzie źródłowym.
4. Kopie zapasowe szyfrowane w spoczynku.

D. Dostępność i kopie zapasowe

1. Codzienne automatyczne kopie zapasowe bazy danych i plików, przechowywane w UE, z retencją [30] dni.
2. Okresowy (co najmniej [kwartalny]) test odtworzenia kopii zapasowej na środowisku testowym, udokumentowany datą i wynikiem.
3. Monitoring dostępności usługi i alerty; aktualizacje bezpieczeństwa systemu operacyjnego i komponentów instalowane regularnie.
4. Środowisko produkcyjne oddzielone od środowisk deweloperskich i testowych; dane produkcyjne nie są kopiowane do środowisk testowych bez anonimizacji.

E. Rozliczalność i monitorowanie

1. Dziennik aktywności w Aplikacji (utworzenie, zmiana, usunięcie kluczowych obiektów: wycieczek, umów, uczestników, wpłat) z identyfikatorem użytkownika i czasem, dostępny dla Administratora.
2. Logi serwera i aplikacji oraz rejestr błędów prowadzone we własnej infrastrukturze Podmiotu przetwarzającego (bez podprocesora), przechowywane [30] dni; treść danych osobowych uczestników nie trafia do rejestru błędów.
3. Rejestr naruszeń ochrony danych; procedura reakcji na incydent: wykrycie, ograniczenie, ocena, zawiadomienie Administratora w ciągu 48 godzin, działania naprawcze, wnioski.
4. Dostęp administracyjny do serwerów wyłącznie kluczem SSH przez wskazane osoby; konfiguracja infrastruktury utrzymywana jako kod (możliwość odtworzenia i przeglądu zmian).

F. Organizacja

1. Osoby z dostępem do danych: [właściciel Podmiotu przetwarzającego oraz wskazani współpracownicy], objęte zobowiązaniem do poufności.
2. Zasada minimalnego dostępu: dostęp do bazy produkcyjnej tylko na potrzeby diagnostyki i wsparcia, po zgłoszeniu Administratora lub przy awarii, dokumentowany.
3. Przegląd podprocesorów i środków bezpieczeństwa co najmniej raz w roku oraz po każdym istotnym incydencie; niniejszy Załącznik jest aktualizowany po przeglądzie.
4. Kod i migracje bazy danych podlegają kontroli wersji i testom automatycznym przed wdrożeniem, w tym testom izolacji między Kontami.

Załącznik nr 3 — Lista podprocesorów

Lp.	Podprocesor	Rola / zakres	Zakres danych	Lokalizacja	Transfer poza EOG / zabezpieczenia	Status
1	OVH — OVH Sp. z o.o., ul. Swobodna 1, 50-088 Wrocław / OVH SAS, Roubaix, Francja	hosting serwerów, przestrzeń na kopie zapasowe	wszystkie powierzone dane (baza danych, pliki, kopie)	EOG (UE): Polska i Niemcy (Frankfurt)	nie dotyczy	stały
2	Mistral AI — Mistral AI SAS,	funkcje AI: rozpoznawanie	treść przesłanych	EOG (UE)	nie dotyczy	opcjonalny — po

Lp.	Podprocesor	Rola / zakres	Zakres danych	Lokalizacja	Transfer poza EOG / zabezpieczenia	Status
	[15 rue des Halles, 75001 Paryż, Francja], API modeli językowych	treści dokumentów i faktur, wsparcie planowania wycieczek	dokumentów i opis wycieczki; dane nie są wykorzystywane przez dostawcę do trenowania modeli na warunkach API			aktywacji funkcji AI przez Administratora (w Okresie Testowym w limicie)
3	Google — Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Irlandia (Google Workspace)	wysyłka wiadomości e-mail z Aplikacji (aktywacje, potwierdzenia zapisów, wiadomości do uczestników i pilotów zlecone przez Administratora), obsługa skrzynki kontakt@tourflow.pl	adresy e-mail odbiorców, imię i nazwisko, treść wiadomości i załączniki	UE, możliwe przetwarzanie w USA	EU-US Data Privacy Framework, standardowe klauzule umowne w warunkach Google Workspace	stały
4	Cloudflare, Inc. , 101 Townsend St, San Francisco, CA 94107, USA	ochrona formularzy rejestracji, resetu hasła i zapisów online przed automatami (Turnstile) [oraz proxy i zapora sieciowa domeny, jeżeli włączone]	adres IP i dane techniczne przeglądarki osoby korzystającej z formularza [oraz ruch HTTPS w tranzycie]	UE/USA	EU-US Data Privacy Framework, standardowe klauzule umowne	stały
5	Krajowy Integrator Płatności S.A. , plac Andersa 3, 61-894 Poznań (Tpay)	obsługa płatności za Usługę w Samodzielnej rejestracji	dane płatnika (Administrator lub jego reprezentant), kwota, identyfikator Konta; NIE dotyczy danych uczestników	Polska	nie dotyczy	w zakresie płatności działa jako odrębny administrator; od udostępnienia płatności w Panelu
6	[dostawca systemu do fakturowania Podmiotu przetwarzającego — nazwa i adres do uzupełnienia]	wystawianie faktur VAT za Usługę	dane nabywcy (nazwa, adres, NIP, e-mail); NIE dotyczy danych uczestników	Polska	nie dotyczy	stały
7	[zewnętrzny magazyn plików Nextcloud: własna instancja / dostawca]	przechowywanie dokumentów wycieczek w zewnętrznym magazynie	dokumenty wycieczek przesłane przez Administratora	[UE]	nie dotyczy	opcjonalny — wyłącznie Plan Rozszerzony (Warunki Indywidualne)

Podmioty, którym dane mogą być ujawniane na polecenie Administratora, a które nie są podprocesorami:
Ubezpieczeniowy Fundusz Gwarancyjny (przekazanie wykazu umów przez interfejs UFG na polecenie

Administradora; UFG jest odrębnym administratorem), odbiorcy wiadomości e-mail wskazani przez Administratora (uczestnicy, piloci, kontrahenci), **Narodowy Bank Polski** (pobieranie kursów walut — bez przekazywania danych osobowych). Generowanie dokumentów PDF odbywa się w infrastrukturze Podmiotu przetwarzającego (własna instancja) i nie stanowi podpowierzenia.