UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

DPA AI Phone Agent - wersja 1.0, 18 lipca 2026 r.

Metryka dokumentu

Pole	Wartość
Wersja	1.0
Data wejścia w życie	18 lipca 2026 r.
Administrator	Klient zidentyfikowany nazwą prawną, adresem i NIP-em w ukończonej sesji Stripe Checkout lub powiązanym rekordzie Stripe Customer.
Reprezentant Administratora	Osoba, która w imieniu Klienta ukończyła Stripe Checkout, zaakceptowała checkbox Regulaminu obejmującego niniejszą Umowę jako integralny dokument oraz której dane utrwalono w Stripe lub systemie obsługi Klienta.
Procesor	Mateusz Borowiec, prowadzący działalność gospodarczą pod firmą Readnest Mateusz Borowiec, os. gen. Władysława Sikorskiego 80, 32-200 Miechów, NIP: 6591530967, REGON: 387686173.
Usługa	AI Phone Agent - agent telefoniczny AI dla firm usługowych.
Podstawa świadczenia Usługi	Regulamin świadczenia usług AI Phone Agent w wersji zaakceptowanej przez Administratora oraz aktywna subskrypcja Klienta.
Data zawarcia z Administratorem	Czas zarejestrowanej akceptacji checkboxa Regulaminu i DPA w wersjach wskazanych przy zakupie oraz ukończenia właściwej sesji Stripe Checkout.
Adres do zgłoszeń Administratora	Adres email podany w Stripe Checkout lub później wskazany Procesorowi.
Adres do zgłoszeń Procesora	contact@aiphoneagent.pl

Preambuła

1. Administrator korzysta z usługi AI Phone Agent, polegającej na obsłudze połączeń telefonicznych przez agenta AI działającego według instrukcji Administratora.

2. W ramach świadczenia Usługi Procesor może przetwarzać dane osobowe osób dzwoniących do Administratora, klientów i potencjalnych klientów Administratora oraz osób działających po stronie Administratora.

3. Strony zawierają niniejszą umowę powierzenia przetwarzania danych osobowych na podstawie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ("RODO").

4. Umowa uzupełnia Regulamin świadczenia usług AI Phone Agent i obowiązuje w związku z aktywną subskrypcją Usługi przez Administratora.

5. Osoba akceptująca Umowę w Stripe Checkout oświadcza, że jest upoważniona do działania w imieniu Administratora.

1. Definicje

1. Administrator oznacza Klienta zidentyfikowanego w sposób opisany w Metryce dokumentu, który decyduje o celach i sposobach przetwarzania danych osobowych osób dzwoniących do jego firmy oraz innych osób, których dane przekazuje do Usługi.

2. Procesor oznacza Mateusza Borowca prowadzącego działalność gospodarczą pod firmą Readnest Mateusz Borowiec, przetwarzającego Powierzone Dane wyłącznie na udokumentowane polecenie Administratora.

3. Usługa oznacza usługę AI Phone Agent, w szczególności automatyczne odbieranie połączeń telefonicznych, prowadzenie rozmów przez agenta AI, tworzenie transkryptów, podsumowań, rekordów rozmów, powiadomień oraz obsługę prostych procesów, takich jak rezerwacje, zmiany terminów, odwołania wizyt lub przyjmowanie zamówień.

4. Umowa główna oznacza umowę o świadczenie Usługi zawartą zgodnie z Regulaminem świadczenia usług AI Phone Agent.

5. Użytkownik końcowy oznacza osobę fizyczną dzwoniącą do Administratora lub kontaktującą się z Administratorem przez kanał obsługiwany przez Usługę.

6. Powierzone Dane oznaczają dane osobowe przetwarzane przez Procesora w imieniu Administratora w ramach Usługi.

7. Subprocesor oznacza podmiot trzeci przetwarzający Powierzone Dane w imieniu Procesora w celu realizacji Usługi.

8. Pojęcia niezdefiniowane w Umowie mają znaczenie nadane im w RODO.

2. Przedmiot i charakter powierzenia

1. Administrator powierza Procesorowi przetwarzanie Powierzonych Danych w zakresie niezbędnym do świadczenia Usługi.

2. Procesor przyjmuje powierzenie i zobowiązuje się przetwarzać Powierzone Dane wyłącznie:

- w celu świadczenia, utrzymania i zabezpieczenia Usługi oraz rozliczenia jej użycia na podstawie niezbędnych metadanych;
- zgodnie z Umową, Umową główną, Regulaminem, konfiguracją agenta oraz udokumentowanymi instrukcjami Administratora;
- przez okres aktywnej subskrypcji Usługi oraz przez okres potrzebny do wykonania obowiązków zwrotu lub usunięcia zgodnie z sekcją 13, chyba że dalszego przechowywania wymaga prawo Unii Europejskiej lub państwa członkowskiego.

3. Szczegółowy opis przetwarzania zawiera Załącznik 1.

4. Procesor nie staje się administratorem Powierzonych Danych i nie może wykorzystywać ich do własnych celów marketingowych, sprzedaży danych ani profilowania niezwiązanego z Usługą.

5. Dane umowne, rozliczeniowe, podatkowe, dowody akceptacji dokumentów i minimalne dane kontaktowe osób działających po stronie Administratora, które Procesor przetwarza we własnych celach prawnych lub rozliczeniowych, nie są Powierzonymi Danymi z rozmów. Zasady ich przetwarzania określa Polityka prywatności Procesora.

3. Instrukcje Administratora

1. Udokumentowanymi instrukcjami Administratora są:

- Regulamin świadczenia usług AI Phone Agent i niniejsza Umowa;
- konfiguracja agenta AI, w tym prompt, zakres wiedzy, zasady rozmowy, kalendarz, dane kontaktowe, cennik, procedury i wyjątki przekazane przez Administratora;
- ustawienia retencji, nagrywania, przekierowania połączeń i powiadomień ustalone z Administratorem;
- pisemne lub elektroniczne dyspozycje Administratora przesłane na adres Procesora wskazany w Metryce dokumentu.

2. Jeżeli Procesor uzna, że instrukcja Administratora narusza RODO, inne przepisy Unii Europejskiej lub państwa członkowskiego o ochronie danych osobowych, niezwłocznie informuje o tym Administratora przed wykonaniem instrukcji, chyba że prawo zabrania przekazania takiej informacji. Procesor może wstrzymać wykonanie wyłącznie kwestionowanego zakresu instrukcji do czasu jej poprawienia albo zgodnego z prawem potwierdzenia oraz może odmówić wykonania instrukcji, której realizacja byłaby niezgodna z prawem.

3. Administrator odpowiada za zgodność instrukcji z prawem, w tym za podstawę prawną nagrywania rozmów, informowanie Użytkowników końcowych, treść komunikatów, legalność danych przekazywanych do agenta oraz prawidłowość danych biznesowych używanych przez agenta.

4. Obowiązki Procesora

Procesor zobowiązuje się:

1. przetwarzać Powierzone Dane wyłącznie na udokumentowane polecenie Administratora;

2. zapewnić, aby osoby upoważnione do przetwarzania Powierzonych Danych były zobowiązane do zachowania poufności;

3. stosować środki techniczne i organizacyjne opisane w Załączniku 2;

4. pomagać Administratorowi, w rozsądnym i możliwym zakresie, w realizacji praw osób, których dane dotyczą;

5. pomagać Administratorowi w wywiązywaniu się z obowiązków dotyczących bezpieczeństwa przetwarzania, zgłaszania naruszeń, oceny skutków dla ochrony danych i konsultacji z organem nadzorczym, o ile zakres Usługi i informacje dostępne Procesorowi na to pozwalają;

6. prowadzić wewnętrzne informacje potrzebne do wykazania zgodności z niniejszą Umową;

7. usuwać albo zwracać Powierzone Dane zgodnie z sekcją 13;

8. nie przekazywać Powierzonych Danych poza zakres wskazany w Umowie, chyba że wymaga tego prawo lub udokumentowana instrukcja Administratora;

9. nie wykorzystywać Powierzonych Danych do trenowania lub ulepszania modeli na potrzeby własne, innych klientów ani dostawców oraz nie łączyć danych osób dzwoniących między różnymi Administratorami;

10. konfigurować dostępne ustawienia Subprocesorów tak, aby wyłączyć wykorzystywanie Powierzonych Danych do trenowania lub ulepszania modeli. Dopuszczalne pozostaje przetwarzanie niezbędne do wykonania Usługi, bezpieczeństwa, zapobiegania nadużyciom lub spełnienia obowiązku prawnego oraz tworzenie statystyk trwale zanonimizowanych, z których nie można zidentyfikować osoby ani Administratora.

5. Obowiązki Administratora

Administrator zobowiązuje się:

1. posiadać właściwą podstawę prawną przetwarzania Powierzonych Danych, w tym danych przekazywanych do Procesora i Subprocesorów;

2. spełnić obowiązek informacyjny wobec Użytkowników końcowych, w szczególności poinformować ich o rozmowie z systemem AI, nagrywaniu rozmowy, celach przetwarzania, odbiorcach danych oraz przysługujących im prawach;

3. nie przekazywać do Usługi danych szczególnych kategorii, danych karnych ani danych nadmiarowych, chyba że jest to konieczne, legalne, udokumentowane i uzgodnione z Procesorem;

4. utrzymywać aktualność danych przekazywanych do konfiguracji agenta, w szczególności grafiku, oferty, cennika, procedur i zasad obsługi klienta;

5. przekazywać Procesorowi tylko takie dane i instrukcje, które są potrzebne do realizacji Usługi;

6. współpracować z Procesorem przy obsłudze żądań osób, incydentów, reklamacji i kontroli;

7. wskazać aktualny adres email do zgłoszeń dotyczących ochrony danych;

8. przed uruchomieniem nagrywania wskazać cel i podstawę prawną nagrywania oraz alternatywny kanał kontaktu dla osoby, która nie chce korzystać z nagrywanego kanału.

6. Nagrywanie rozmów i informacja o AI

1. Jeżeli konfiguracja Usługi obejmuje nagrywanie, Administrator przed uruchomieniem produkcyjnym określa cel i podstawę prawną nagrywania, zakres obowiązku informacyjnego oraz dostępny sposób kontaktu bez korzystania z nagrywanego kanału.

2. Procesor zapewnia, aby komunikat startowy zgodny z zatwierdzoną konfiguracją jasno informował, że Użytkownik końcowy kontaktuje się z systemem AI oraz - jeżeli nagrywanie jest aktywne - że rozmowa jest nagrywana. Komunikat musi odpowiadać faktycznej konfiguracji.

3. Samo kontynuowanie połączenia albo jego zakończenie nie jest przez Procesora traktowane jako automatyczne wykazanie ważnej zgody. Jeżeli Administrator opiera przetwarzanie na zgodzie, odpowiada za spełnienie warunków jej dobrowolności, konkretności, świadomości i możliwości wycofania.

4. W razie sprzeciwu wobec nagrywania Agent AI nie powinien dalej zbierać danych i przekazuje Użytkownikowi końcowemu uzgodniony z Administratorem alternatywny kanał kontaktu.

5. Administrator posiada własną politykę prywatności albo informację RODO dla osób dzwoniących do jego firmy, obejmującą korzystanie z Usługi. Niniejsza Umowa nie zastępuje tej informacji.

6. Procesor może rekomendować treść komunikatu startowego, ale ostateczna odpowiedzialność za zgodność celu, podstawy prawnej i informacji Administratora spoczywa na Administratorze.

7. Bezpieczeństwo przetwarzania

1. Procesor wdraża i utrzymuje odpowiednie środki techniczne i organizacyjne, uwzględniając stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych.

2. Minimalny zestaw środków bezpieczeństwa obejmuje Załącznik 2. Środki podlegają przeglądowi po istotnej zmianie architektury, Subprocesora, rodzaju danych albo po incydencie.

3. Administrator przyjmuje do wiadomości, że Usługa korzysta z zewnętrznych systemów AI, telefonii, automatyzacji i przechowywania danych. Procesor dobiera Subprocesorów, którzy zobowiązują się stosować odpowiednie środki bezpieczeństwa i zawierają właściwe umowy dotyczące danych.

4. Procesor może aktualizować środki bezpieczeństwa, jeżeli nie obniża to istotnie ogólnego poziomu ochrony Powierzonych Danych.

8. Subprocesorzy

1. Administrator udziela Procesorowi ogólnej zgody na korzystanie z Subprocesorów wymienionych w aktualnym Załączniku 3.

2. Procesor zawiera z każdym bezpośrednim Subprocesorem umowę nakładającą w zakresie Powierzonych Danych zasadniczo te same obowiązki ochrony danych, które wynikają z niniejszej Umowy i art. 28 RODO.

3. Procesor pozostaje wobec Administratora w pełni odpowiedzialny za wykonanie obowiązków ochrony danych przez swoich bezpośrednich Subprocesorów w zakresie wymaganym przez art. 28 ust. 4 RODO.

4. Procesor może dodać albo zmienić Subprocesora, jeżeli jest to potrzebne do świadczenia, utrzymania, zabezpieczenia lub rozwoju Usługi.

5. O planowanej istotnej zmianie Procesor informuje Administratora emailowo i aktualizuje publiczną listę co najmniej 30 dni przed zmianą. W pilnej zmianie wymaganej bezpieczeństwem lub prawem informuje bez zbędnej zwłoki, podając przyczynę i ograniczając zmianę do koniecznego zakresu.

6. Administrator może w terminie 14 dni zgłosić uzasadniony sprzeciw związany z ochroną danych. Strony w dobrej wierze szukają rozsądnej alternatywy. Gdy jej brak, każda ze Stron może zakończyć część Usługi zależną od danego Subprocesora bez dodatkowej kary; opłata pobrana z góry za niedostarczony okres podlega proporcjonalnemu rozliczeniu.

7. Dalsi podprocesorzy bezpośrednich Subprocesorów są objęci obowiązkami i odpowiedzialnością wynikającymi z umów Procesora z tymi dostawcami. Procesor monitoruje udostępniane przez nich listy i powiadomienia o zmianach.

8. Lista dostawców płatności, hostingu strony marketingowej i narzędzi sprzedażowych może być szersza niż lista Subprocesorów Usługi. Tacy dostawcy nie przetwarzają standardowo danych Użytkowników końcowych w ramach niniejszego powierzenia, chyba że zostaną wyraźnie włączeni do konkretnej konfiguracji Usługi.

9. Transfery danych poza EOG

1. Administrator upoważnia Procesora do przekazywania Powierzonych Danych poza Europejski Obszar Gospodarczy wyłącznie, gdy jest to niezbędne do świadczenia Usługi i zapewniono ważny mechanizm z rozdziału V RODO.

2. Transfery poza EOG mogą odbywać się w szczególności na podstawie:

- decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony, w tym EU-US Data Privacy Framework, jeżeli dany odbiorca jest aktywnie certyfikowany;
- standardowych klauzul umownych Komisji Europejskiej;
- innych mechanizmów dopuszczonych przez RODO.

3. Aktualny bezpośredni odbiorca, rola, typowa lokalizacja i mechanizm ochrony są wskazane w Załączniku 3. Procesor uwzględnia publicznie dostępne DPA, listy subprocesorów i mechanizmy transferowe tych dostawców.

4. Jeżeli dany Subprocesor przestanie zapewniać właściwy mechanizm transferowy, Procesor podejmie rozsądne działania naprawcze, takie jak zmiana konfiguracji, ograniczenie zakresu danych, wybór alternatywnego dostawcy albo rozwiązanie Usługi w zakresie, w którym dalsze świadczenie byłoby niezgodne z prawem.

10. Żądania osób, których dane dotyczą

1. Jeżeli Procesor otrzyma żądanie osoby, której dane dotyczą, związane z Powierzonymi Danymi, Procesor bez zbędnej zwłoki przekaże żądanie Administratorowi, o ile będzie w stanie powiązać żądanie z Administratorem.

2. Procesor nie odpowiada merytorycznie na żądanie osoby, chyba że Administrator udzieli mu takiej instrukcji albo odpowiedź jest wymagana prawem.

3. Procesor, uwzględniając charakter przetwarzania, pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne w realizacji żądań dostępu, sprostowania, usunięcia, ograniczenia, przenoszenia danych, sprzeciwu lub cofnięcia zgody. Pomoc nie jest ograniczona wyłącznie do funkcji samoobsługowych, jeżeli dane pozostają pod kontrolą Procesora. Nadzwyczajne prace wykraczające poza standardową obsługę mogą być odpłatne tylko po uprzednim uzgodnieniu i nie ograniczają obowiązków, których Procesor nie może wyłączyć na podstawie RODO.

4. Administrator odpowiada za terminową i kompletną odpowiedź wobec osoby, której dane dotyczą.

11. Naruszenia ochrony danych osobowych

1. Procesor informuje Administratora o naruszeniu ochrony Powierzonych Danych bez zbędnej zwłoki po powzięciu wiadomości o naruszeniu, w miarę możliwości nie później niż w ciągu 48 godzin. Termin ten nie ogranicza obowiązku wcześniejszego zgłoszenia, gdy dostępne informacje pozwalają racjonalnie uznać, że doszło do naruszenia.

2. Zgłoszenie zawiera informacje dostępne Procesorowi w chwili zgłoszenia, w szczególności:

- opis charakteru naruszenia;
- kategorie i przybliżoną liczbę osób lub rekordów, których dotyczy naruszenie, jeżeli są znane;
- możliwe konsekwencje naruszenia;
- działania podjęte albo proponowane w celu ograniczenia skutków naruszenia;
- punkt kontaktowy do dalszej komunikacji.

3. Jeżeli pełne informacje nie są dostępne od razu, Procesor przekazuje je etapami bez zbędnej zwłoki.

4. Administrator odpowiada za ocenę, czy naruszenie wymaga zgłoszenia Prezesowi Urzędu Ochrony Danych Osobowych albo zawiadomienia osób, których dane dotyczą.

12. DPIA, konsultacje i branże podwyższonego ryzyka

1. Procesor pomaga Administratorowi w rozsądnym zakresie przy ocenie skutków dla ochrony danych i konsultacjach z organem nadzorczym, jeżeli charakter konfiguracji Usługi tego wymaga.

2. Standardowa Usługa nie jest skonfigurowana do celowego zbierania danych szczególnych kategorii ani danych o wyrokach i naruszeniach prawa. Agent powinien ograniczać pytania do danych organizacyjnych potrzebnych do wykonania uzgodnionej czynności.

3. Celowe przetwarzanie danych zdrowotnych lub innych danych szczególnych kategorii wymaga przed uruchomieniem odrębnej pisemnej instrukcji, uzgodnionej konfiguracji minimalizującej dane, potwierdzenia podstawy z art. 9 RODO, oceny ryzyka i - jeżeli jest wymagana - DPIA oraz dodatkowego załącznika branżowego.

4. Incydentalna, spontaniczna wypowiedź Użytkownika końcowego zawierająca dane szczególnych kategorii nie może zostać całkowicie wykluczona. Agent nie powinien jednak dopytywać ani wykorzystywać takiej informacji poza niezbędnym przekazaniem sprawy zgodnie z instrukcją Administratora.

5. Dane dzieci lub inne dane podwyższonego ryzyka wymagają przed uruchomieniem dodatkowej instrukcji, minimalizacji i oceny zgodności procesu z prawem.

13. Zwrot, usunięcie i retencja danych

1. W okresie świadczenia Usługi okres dostępności nagrań, transkryptów i rekordów rozmów wynika z Planu albo udokumentowanej konfiguracji Administratora. Procesor stosuje tę retencję we wszystkich zwykłych, aktywnie dostępnych systemach znajdujących się pod jego kontrolą:

- Starter: do 30 dni;
- Business: do 60 dni;
- Business Pro: do 90 dni;
- konfiguracja indywidualna: zgodnie z ustaleniami Stron.

2. Po zakończeniu Usługi Procesor, według wyboru Administratora, zwraca Powierzone Dane, a następnie usuwa pozostałe kopie, albo usuwa Powierzone Dane bez zwrotu. Jeżeli Administrator nie dokona wyboru do dnia zakończenia, Procesor usuwa dane.

3. Procesor uruchamia usunięcie bez zbędnej zwłoki i usuwa dane ze zwykłych, aktywnie dostępnych systemów nie później niż w ciągu 30 dni od zakończenia Usługi. Potwierdza wykonanie na żądanie Administratora.

4. Resztkowe kopie w odizolowanych kopiach zapasowych lub logach bezpieczeństwa Subprocesora mogą pozostać wyłącznie przez udokumentowany okres techniczny dostawcy wskazany lub podlinkowany w Załączniku 3. Nie mogą być w tym czasie zwykle dostępne ani używane do innych celów i są usuwane lub nadpisywane zgodnie z cyklem dostawcy. Po ewentualnym odtworzeniu kopii podlegają ponownemu usunięciu.

5. Dalsze zachowanie Powierzonych Danych jest dopuszczalne tylko, gdy obowiązek przechowywania wynika z prawa Unii Europejskiej lub państwa członkowskiego. Procesor informuje Administratora o podstawie i zakresie, o ile prawo tego nie zabrania.

6. Dane umowne, rozliczeniowe, podatkowe, dowody akceptacji i minimalne dane kontaktowe przetwarzane przez Procesora jako odrębnego administratora nie są Powierzonymi Danymi z rozmów. Ich zasady retencji określa Polityka prywatności. Treść rozmów, audio, transkrypty, podsumowania i payloady nie są zachowywane bezterminowo w celu zabezpieczenia roszczeń po zakończeniu powierzenia.

14. Audyt i wykazanie zgodności

1. Procesor udostępnia informacje niezbędne do wykazania zgodności z art. 28 RODO oraz umożliwia i przyczynia się do audytów, w tym inspekcji, prowadzonych przez Administratora albo upoważnionego audytora.

2. Rutynowy audyt rozpoczyna się od dokumentów i spotkania zdalnego, odbywa się nie częściej niż raz na 12 miesięcy i po co najmniej 14 dniach zawiadomienia.

3. Ograniczenia z ust. 2 nie obowiązują w razie naruszenia dotyczącego Administratora, wiarygodnego podejrzenia istotnej niezgodności albo żądania organu nadzorczego.

4. Audyt odbywa się w godzinach pracy, z zachowaniem poufności, bezpieczeństwa i praw innych klientów. Audytor nie może uzyskać dostępu do danych innych Administratorów ani tajemnic niezwiązanych z zakresem audytu.

5. Koszt audytu ponosi Administrator, chyba że audyt wykaże istotne naruszenie Umowy lub RODO przez Procesora.

15. Poufność

1. Strony zobowiązują się zachować w poufności informacje techniczne, organizacyjne, biznesowe i prawne uzyskane w związku z Umową.

2. Procesor ogranicza dostęp do Powierzonych Danych do osób i narzędzi, które potrzebują dostępu w celu świadczenia, utrzymania, zabezpieczenia lub rozliczenia Usługi.

3. Obowiązek poufności trwa także po zakończeniu Umowy.

16. Odpowiedzialność

1. Odpowiedzialność Stron z tytułu niniejszej Umowy podlega ograniczeniom odpowiedzialności przewidzianym w Umowie głównej lub Regulaminie, o ile bezwzględnie obowiązujące przepisy prawa nie stanowią inaczej.

2. Administrator odpowiada za zgodność z prawem celów i podstaw przetwarzania, spełnienie obowiązku informacyjnego wobec Użytkowników końcowych, treść instrukcji oraz dane przekazywane do Usługi.

3. Procesor odpowiada za przetwarzanie Powierzonych Danych niezgodnie z Umową, jeżeli działał poza zgodnymi z prawem instrukcjami Administratora albo naruszył obowiązki procesora wynikające z RODO.

4. Ograniczenie odpowiedzialności nie ma zastosowania do szkody wyrządzonej umyślnie ani w zakresie, w którym bezwzględnie obowiązujące przepisy nie pozwalają na ograniczenie, w szczególności do odpowiedzialności i roszczeń zwrotnych wynikających z art. 82 RODO. Żaden zapis nie wyłącza obowiązków Procesora wynikających bezpośrednio z RODO.

17. Czas obowiązywania

1. Umowa obowiązuje wobec danego Administratora od zarejestrowanej Daty zawarcia z Administratorem wskazanej w Metryce dokumentu.

2. Umowa obowiązuje przez czas trwania aktywnej subskrypcji Usługi oraz przez okres potrzebny do wykonania obowiązków dotyczących zwrotu, usunięcia, audytu lub obsługi incydentów.

3. Zakończenie aktywnej subskrypcji Usługi powoduje zakończenie niniejszej Umowy, z zastrzeżeniem obowiązków, które ze swojej natury trwają po zakończeniu współpracy.

18. Zawarcie elektroniczne, wersjonowanie i postanowienia końcowe

1. Niniejsza Umowa stanowi integralną część Umowy głównej. W razie sprzeczności między niniejszą Umową a Umową główną w zakresie przetwarzania danych osobowych pierwszeństwo ma niniejsza Umowa.

2. Umowa zostaje zawarta elektronicznie, gdy osoba działająca w imieniu Administratora zaakceptuje wymagany checkbox Regulaminu, który wskazuje niniejszą Umowę jako integralny dokument w określonej wersji, oraz ukończy właściwą sesję Stripe Checkout.

3. Procesor utrwala dowód zawarcia Umowy obejmujący co najmniej identyfikator sesji Stripe Checkout, identyfikator Klienta Stripe, dane identyfikujące Administratora, czas akceptacji, zaakceptowaną wersję Regulaminu i DPA oraz informację o wymaganej zgodzie.

4. Każda wersja Umowy posiada odrębny numer i trwały adres archiwalny. Aktualna wersja jest dostępna pod adresem https://aiphoneagent.pl/dpa, a wersja 1.0 pod adresem https://aiphoneagent.pl/dpa/v1.0.

5. Istotna zmiana obowiązków Stron, zakresu lub celu przetwarzania wymaga odrębnej, wyraźnej akceptacji nowej wersji przez Administratora, zanim zacznie ona obowiązywać wobec tego Administratora. Zmiany Subprocesorów są dokonywane

zgodnie z sekcją 8.

6. W sprawach nieuregulowanych zastosowanie ma prawo polskie oraz RODO.

7. Spory wynikające z Umowy będą rozstrzygane przez sąd właściwy dla siedziby Procesora, chyba że Regulamin świadczenia usług AI Phone Agent przewiduje inne właściwe forum.

Załącznik 1 - Szczegóły przetwarzania

Element	Opis
Przedmiot przetwarzania	Obsługa połączeń telefonicznych i procesów komunikacyjnych Administratora przez agenta AI.
Cel przetwarzania	Odbieranie połączeń, prowadzenie rozmów, umawianie, przesuwanie i odwoływanie wizyt, przyjmowanie zamówień, udzielanie informacji, tworzenie podsumowań, wysyłka powiadomień, raportowanie, obsługa reklamacji, kontrola i korekta konfiguracji danego Administratora oraz bezpieczeństwo Usługi.
Charakter przetwarzania	Zbieranie, utrwalanie, transkrypcja, analiza, strukturyzacja, przechowywanie, odczyt, modyfikacja, przekazywanie między systemami, usuwanie i anonimizacja danych.
Czas przetwarzania	Czas trwania aktywnej subskrypcji Usługi oraz okres retencji określony w Umowie, Planie, konfiguracji lub przepisach prawa.
Kategorie osób	Użytkownicy końcowi dzwoniący do Administratora, klienci i potencjalni klienci Administratora, osoby odwołujące lub rezerwujące wizyty, osoby składające zamówienia, osoby kontaktowe po stronie Administratora, pracownicy lub współpracownicy Administratora wskazani w konfiguracji.
Kategorie danych	Numer telefonu, imię i nazwisko albo imię, nazwa firmy, dane kontaktowe, treść rozmowy, nagranie audio, transkrypt, metadane połączenia, data i godzina kontaktu, dane rezerwacji lub zamówienia, preferencje terminu, informacje przekazane dobrowolnie w rozmowie, status obsługi, notatki i podsumowania.
Dane szczególnych kategorii	Nie są celowo zbierane w standardowej Usłudze. Mogą pojawić się incydentalnie, jeżeli Użytkownik końcowy poda je spontanicznie. Ich celowe zbieranie wymaga odrębnej instrukcji, dodatkowego załącznika branżowego, minimalizacji, potwierdzenia podstawy z art. 9 RODO i oceny ryzyka.
Dane dzieci	Nie są zakładanym elementem standardowej Usługi. Jeżeli Administrator obsługuje dzieci lub ich opiekunów, musi przekazać Procesorowi dodatkowe instrukcje i ocenić zgodność takiego procesu z prawem.
Źródło danych	Użytkownicy końcowi, Administrator, systemy Administratora, konfiguracja agenta i systemy używane do świadczenia Usługi.
Odbiorcy danych	Procesor, upoważnione osoby Procesora, Subprocesorzy wskazani w Załączniku 3, Administrator oraz osoby wskazane przez Administratora jako odbiorcy powiadomień lub raportów.

Załącznik 2 - Minimalne środki techniczne i organizacyjne

1. Kontrola dostępu:

- dostęp do kont administracyjnych tylko dla upoważnionych osób;
- stosowanie silnych, unikalnych haseł oraz wymaganie uwierzytelniania wieloskładnikowego dla kont mających dostęp do Powierzonych Danych, wszędzie, gdzie usługa je wspiera; konto bez włączonego MFA nie może być używane do produkcyjnego przetwarzania danych Administratora;
- ograniczanie dostępu i uprawnień integracji do niezbędnego zakresu;
- przegląd dostępów po zmianie osoby, dostawcy lub zakresu Usługi.

2. Separacja klientów i konfiguracji:

- używanie stabilnych identyfikatorów client_id i agent_id;
- unikanie routingu automatyzacji po samej nazwie firmy;
- rozdzielanie konfiguracji agentów, folderów i rekordów operacyjnych w sposób ograniczający ryzyko pomyłki między klientami.

3. Bezpieczeństwo transmisji:

- korzystanie z HTTPS/TLS przy komunikacji z panelami, API i webhookami;
- zabezpieczanie endpointów formularzy i webhooków podpisem dostawcy, sekretem albo równoważnym mechanizmem kontroli dostępu;
- odrzucanie nieprawidłowych typów zdarzeń, brakujących kluczy routingu i nadmiernych payloadów.

4. Ograniczenie danych:

- zbieranie danych potrzebnych do obsługi rozmowy, rezerwacji, zamówienia lub powiadomienia;
- unikanie celowego zbierania danych szczególnych kategorii w standardowej Usłudze;
- ograniczanie danych w promptach, bazach wiedzy, arkuszach, powiadomieniach i logach do informacji potrzebnych agentowi i odbiorcy.

5. Retencja:
   - stosowanie okresów retencji nagrań i transkryptów zgodnych z Planem lub indywidualną konfiguracją;
   - usuwanie albo anonimizacja danych po upływie retencji i po zakończeniu współpracy;
   - dokumentowanie żądań oraz potwierdzeń usunięcia;
   - kontrola ustawień retencji u Subprocesorów.
6. Monitorowanie i jakość:
   - ręczny monitoring tylko w niezbędnym zakresie, przez osoby upoważnione i w ramach retencji Administratora;
   - analiza błędów wyłącznie w celu poprawy konfiguracji danego Administratora i bezpieczeństwa Usługi;
   - nieużywanie danych klienta do publicznych materiałów marketingowych bez zgody.
7. Zarządzanie sekretami:
   - przechowywanie kluczy API i tokenów poza publicznym repozytorium;
   - rotacja sekretów w razie podejrzenia ujawnienia;
   - niewysyłanie sekretów w logach, dokumentacji publicznej ani powiadomieniach.
8. Incydenty:
   - procedura kontaktu emailowego przy incydentach;
   - rejestr incydentów, żądań osób i działań naprawczych;
   - współpraca z Administratorem przy ocenie skutków incydentu.
9. Zarządzanie zmianą:
   - przegląd środków po istotnej zmianie architektury, Subprocesora lub kategorii danych;
   - monitorowanie publicznych list Subprocesorów i komunikatów bezpieczeństwa;
   - test podstawowych scenariuszy przed aktywacją produkcyjną agenta.

Załącznik 3 - Lista Subprocesorów Usługi

Subprocesor umowny	Lokalizacja / przetwarzanie	Rola w Usłudze	Kategorie danych	Mechanizm ochrony / uwagi
Eleven Labs, Inc.	USA; możliwe przetwarzanie globalne przez dalszych podprocesorów	Platforma głosowa AI, orkiestracja rozmów, STT, TTS, transkrypcje i logi rozmów.	Nagrania, transkrypty, tekst rozmowy, metadane połączeń i identyfikatory agenta.	DPA ElevenLabs; DPF lub SCC zależnie od odbiorcy. Używanie nowych danych do ulepszania modeli jest wyłączone na koncie Procesora. Retencja jest ustawiana per agent.
OpenAI Ireland Limited	Irlandia; możliwe transfery zgodnie z DPA i listą podprocesorów	Model językowy używany przez bezpośrednie połączenie Custom LLM.	Prompt, kontekst i tekst rozmowy oraz dane przekazane w wypowiedzi.	DPA OpenAI; dane API nie są domyślnie używane do trenowania, a standardowe logi bezpieczeństwa mogą być przechowywane do 30 dni.
Twilio Ireland Limited	Irlandia; możliwe transfery zgodnie z DPA i listą podprocesorów	Telefonia, routing połączeń, metadane telekomunikacyjne i numeracja.	Numery telefonów, identyfikatory i metadane połączeń; audio tylko jeżeli funkcja nagrywania Twilio zostanie włączona.	DPA Twilio; mechanizmy z rozdziału V RODO zależnie od odbiorcy.
Google Cloud Poland Sp. z o.o. albo podmiot wskazany w dokumentach konta Google Workspace	Polska / EOG; możliwe przetwarzanie globalne przez podprocesorów Google	Google Workspace, Sheets, Drive i Gmail do rekordów operacyjnych i powiadomień.	Podsumowania, rekordy rozmów, linki i dane kontaktowe; audio tylko przy świadomie włączonej archiwizacji.	Google Cloud/Workspace DPA i tabela podmiotów Google. Właściwy podmiot jest potwierdzany dokumentem konta lub fakturą.
Celonis, Inc. albo podmiot wskazany w dokumentach konta Make	USA; możliwe przetwarzanie globalne przez podprocesorów Make	Automatyzacje, webhooki, mapowanie danych oraz przesyłanie rekordów do arkuszy i emaili.	Payload webhooka, dane rozmowy, rezerwacji lub zamówienia i logi operacji.	DPA Make; DPF lub SCC zależnie od odbiorcy. Właściwy podmiot jest potwierdzany dokumentem konta.
Netlify, Inc.	USA; możliwe przetwarzanie globalne przez podprocesorów Netlify	Hosting funkcji pośredniczącej, która weryfikuje podpis webhooka ElevenLabs i przekazuje prawidłowy payload do Make.	Payload post-call, w tym identyfikatory, metadane, transkrypt, podsumowanie i inne dane przekazane w zdarzeniu; techniczne logi wykonania.	DPA Netlify; DPF lub SCC zależnie od odbiorcy. Funkcja nie zapisuje payloadu w własnej bazie aplikacji, a sekrety są przechowywane poza repozytorium.

Dostawcy poza standardowym zakresem Powierzonych Danych

Dostawca	Status
Stripe Payments Europe, Limited i właściwe podmioty Stripe	Dostawca płatności i rozliczeń. Standardowo przetwarza dane Klienta jako płatnika, a nie dane Użytkowników końcowych powierzone w ramach Usługi.
Google Analytics	Analityka strony marketingowej po zgodzie użytkownika strony. Nie jest elementem standardowego powierzenia danych z rozmów telefonicznych.

Historia wersji

Wersja	Obowiązuje od	Status
1.0	18 lipca 2026 r.	Aktualna wersja. Brak wcześniejszych wersji.