Umowa o powierzeniu przetwarzania danych osobowych

zgodnie z art. 28 RODO

Data publikacji aktualnej wersji: 06.08.2026

Jedynie niemiecka wersja tego dokumentu ma moc prawną. Tłumaczenie ma charakter wyłącznie informacyjny.

Niniejsza polska wersja obejmuje postanowienia mające zastosowanie do klientów z siedzibą w Polsce. Pominięto wyłącznie postanowienia zaadresowane wprost do Zleceniodawców z siedzibą w Szwajcarii (Aneks dla klientów z siedzibą w Szwajcarii oraz odnoszące się do niego wyjaśnienia), które nie mogą mieć zastosowania do klientów z Polski. Pełna wersja niemiecka pozostaje dostępna na stronie.

Administrator danych

Klient odpowiedzialny za przetwarzanie
(dalej: Zleceniodawca)

Podmiot przetwarzający

fonio GmbH
Neustiftgasse 73-75/3/7
1070 Wiedeń
Austria
(dalej: Zleceniobiorca)

O ile Zleceniodawca i Zleceniobiorca nie postanowią inaczej, niniejsza umowa powierzenia przetwarzania stanowi integralną część ogólnych warunków handlowych Zleceniobiorcy, dostępnych pod adresem https://www.fonio.ai/agbs. Niniejsza umowa obowiązuje między Zleceniodawcą a Zleceniobiorcą zawsze wtedy, gdy Zleceniobiorca przetwarza dane osobowe na zlecenie Zleceniodawcy w ramach świadczenia swoich usług.

1. TŁO I SPECYFIKACJA PRZETWARZANIA DANYCH

1.1 Zleceniobiorca jest przedsiębiorstwem oferującym następujące usługi:

- Konfiguracja, zarządzanie i udostępnianie asystenta telefonicznego AI za pośrednictwem aplikacji internetowej B2B fonio.ai

1.2 Zleceniodawca jest przedsiębiorstwem, które zamierza skorzystać z usług Zleceniobiorcy w wymienionych obszarach.

1.3 Niniejsza umowa powierzenia przetwarzania określa warunki przetwarzania danych osobowych przez Zleceniobiorcę za zgodą Zleceniodawcy, zgodnie z Rozporządzeniem o Ochronie Danych Osobowych (RODO). Zleceniobiorca działa jako podmiot przetwarzający w rozumieniu RODO.

2. CHARAKTER, CEL, PRZEDMIOT I PODSTAWA PRAWNA PRZETWARZANIA DANYCH

2.1 Usługi Zleceniobiorcy zostały opisane w ogólnych warunkach handlowych Zleceniobiorcy, dostępnych pod adresem https://www.fonio.ai/agbs.

2.2 W toku świadczenia usług Zleceniodawca udostępnia Zleceniobiorcy dane osobowe niezbędne do ich wykonania, w sposób odpowiedni dla danego przypadku. Może to nastąpić drogą elektroniczną lub fizyczną, poprzez rozmowy i analizy, wykonywanie innych czynności uregulowanych umownie, ustnie lub za

pośrednictwem narzędzi programistycznych.

2.3 Przetwarzanie danych osobowych może polegać w szczególności na organizowaniu, porządkowaniu, przechowywaniu, a także w stosownych przypadkach na dostosowywaniu lub modyfikowaniu, pobieraniu, łączeniu, ograniczaniu, usuwaniu, zestawianiu, kopiowaniu, ukrywaniu, powiązywaniu, analizowaniu, odczytywaniu, odbieraniu, przesyłaniu i aktualizowaniu, w zakresie niezbędnym do świadczenia uzgodnionych usług.

2.4 Celem przetwarzania jest świadczenie usług na rzecz Zleceniodawcy w zakresie określonym umownie.

2.5 Zleceniobiorca nie jest zobowiązany do badania zgodności z prawem przetwarzania danych realizowanego przez Zleceniodawcę.

3. DANE OSOBOWE ORAZ KATEGORIE OSÓB, KTÓRYCH DANE DOTYCZĄ

3.1 W ramach uzgodnionych usług mogą być przetwarzane dane osobowe niezbędne do ich świadczenia. W szczególności mogą to być następujące dane:

- Dane związane z jakością usług
- Dane rozliczeniowe
- Numery telefonów
- Dane kontaktowe
- Dane o zachowaniu użytkowników i interakcjach
- Informacje o urządzeniu
- Informacje o przeglądarce
- Dane identyfikacyjne
- Techniczne dane dostępowe (na przykład klucze API)
- Dane z rozmów telefonicznych
- Wszelkie dane, które uczestnicy rozmowy samodzielnie przekazują AI w jej trakcie
- Dane dotyczące spotkań i wizyt
- Dane konfiguracyjne
- Dane głosowe
- Informacje przekazywane pocztą elektroniczną
- Dane komunikacyjne
- Informacje techniczne
- Informacje przekazywane w formie swobodnego tekstu
- Dane płatnicze
- Dane z logów
- Metadane telefoniczne
- Adresy IP
- Preferencje osobiste
- Pliki cookie i podobne technologie
- Prompty AI oraz inne informacje związane z AI
- Dane techniczne dotyczące błędów
- Dane uwierzytelniające
- Zachowanie użytkownika istotne dla analizy błędów

- Dane abonamentowe
- Dane transakcyjne

3.2 Przetwarzanie obejmuje co do zasady wszystkie szczególne kategorie danych osobowych (art. 9 RODO) niezbędne do świadczenia uzgodnionych usług. W szczególności w ramach świadczenia uzgodnionych usług (na przykład dla gabinetów lekarskich) mogą być przetwarzane następujące szczególne kategorie danych osobowych:

- Dane dotyczące zdrowia

3.3 Przetwarzanie obejmuje co do zasady wszystkie kategorie osób, których dane dotyczą, niezbędne do świadczenia uzgodnionych usług. W szczególności należą do nich następujące kategorie:

- Klienci
- Podmioty trzecie związane umową z Klientem
- Pracownicy Klienta
- Klienci Klienta
- Partnerzy Klienta
- Dostawcy Klienta

3.4 Ze względu na charakter uzgodnionych usług Zleceniodawca przyjmuje do wiadomości, że Zleceniobiorca w znacznej mierze nie może ani weryfikować, ani aktualizować listy kategorii osób, których dane dotyczą. Zleceniodawca zobowiązuje się w związku z tym informować Zleceniobiorcę o wszelkich niezbędnych zmianach tej listy.

3.5 Zleceniobiorca będzie przetwarzał dane osobowe Zleceniodawcy w odniesieniu do wszystkich wymienionych powyżej osób zgodnie z uzgodnionymi usługami. Jeżeli zmiany listy kategorii osób, których dane dotyczą, spowodują konieczność zmiany uzgodnionych operacji przetwarzania, Zleceniodawca wyda Zleceniobiorcy odpowiednie dodatkowe polecenia.

3.6 Brak identyfikacji i weryfikacji głosowej

(a) Zleceniobiorca w ramach uzgodnionych usług nie prowadzi identyfikacji głosowej ani weryfikacji głosowej. W szczególności nie tworzy, nie przechowuje ani nie porównuje wzorców głosu („voiceprints”, szablonów głosowych) i nie stosuje rozwiązań technicznych ukierunkowanych na jednoznaczną identyfikację ani na rozpoznawanie osoby fizycznej po głosie w kolejnych rozmowach. Dane głosowe są przetwarzane wyłącznie w celu wprowadzania i odtwarzania mowy oraz transkrypcji (speech-to-text / text-to-speech). Uwarunkowane technicznie rozróżnianie wypowiedzi w obrębie pojedynczej rozmowy (na przykład oddzielenie dzwoniącego od asystenta) nie służy identyfikacji i nie umożliwia rozpoznania osoby poza tą rozmową.

(b) W ocenie własnej Zleceniobiorcy przetwarzane dane głosowe nie stanowią zatem danych biometrycznych służących jednoznacznej identyfikacji osoby fizycznej w rozumieniu art. 4 pkt 14 i art. 9 ust. 1 RODO. Punkt 3.6 lit. a zawiera opis stanu faktycznego, a lit. b stanowisko prawne Zleceniobiorcy; nie wiąże się z tym gwarancja ani zapewnienie w rozumieniu prawnym. Kwalifikacja prawna poszczególnych operacji przetwarzania zleconych przez Zleceniodawcę należy do Zleceniodawcy jako administratora danych; punkt 2.5 pozostaje nienaruszony.

(c) Nie narusza to faktu, że przetwarzanie może z innych przyczyn obejmować szczególne kategorie danych osobowych w rozumieniu art. 9 RODO, w szczególności dane dotyczące zdrowia (punkt 3.2), oraz że treść rozmów może pozwalać na wyciąganie wniosków co do takich danych.

4. WARUNKI PRZETWARZANIA DANYCH

4.1 Zleceniobiorca zobowiązuje się przestrzegać wszystkich wymogów RODO przez cały okres świadczenia usług.

4.2 Zleceniobiorca zobowiązuje się przetwarzać dane osobowe wyłącznie na pisemne polecenie w formie umowy ze Zleceniodawcą. Odstępstwa od tych poleceń wymagają uprzedniej pisemnej zgody Zleceniodawcy.

4.3 Zleceniobiorca przetwarza dane osobowe zgodnie z zasadą minimalizacji danych określoną w art. 5 ust. 1 lit. c RODO, a więc wyłącznie w zakresie niezbędnym do świadczenia uzgodnionych usług.

4.4 Dostęp do danych osobowych Zleceniodawcy przyznawany jest wyłącznie osobom, które potrzebują go na podstawie postanowień umownych lub przepisów prawa.

4.5 Wszystkie osoby po stronie Zleceniobiorcy, które mają dostęp do danych osobowych Zleceniodawcy, zobowiązane są do zachowania poufności. Obowiązek zachowania poufności osób odpowiedzialnych za obieg danych pozostaje w mocy również po zakończeniu ich działalności i odejściu ze Zleceniobiorcy.

Jeżeli Zleceniodawca podlega ustawowemu obowiązkowi zachowania tajemnicy zawodowej, dodatkowo obowiązuje oświadczenie o zachowaniu poufności i ochronie danych wskazane w Załączniku 4, w wersji przewidzianej dla państwa siedziby Zleceniodawcy; jest ono dostępne w dokładnym brzmieniu pod adresem wskazanym w Załączniku 4. Uznaje się je za uzgodnione z chwilą zawarcia umowy, bez konieczności odrębnego porozumienia ani podpisu; kontrasygnata następuje na życzenie Zleceniodawcy, nie jest jednak wymagana dla skuteczności.

4.6 Zleceniobiorca jest zobowiązany wdrożyć i utrzymywać wszelkie odpowiednie, adekwatne i zgodne ze stanem techniki środki techniczne i organizacyjne w celu zapewnienia dostępności, poufności i integralności danych osobowych. Lista uzgodnionych środków technicznych i organizacyjnych stanowi Załącznik 1 do niniejszej umowy.

4.7 Zleceniobiorca wspiera Zleceniodawcę w wypełnianiu jego obowiązków wynikających z RODO, w szczególności w zakresie praw osób, których dane dotyczą.

4.8 O ile nie stoją temu na przeszkodzie przepisy prawa, Zleceniobiorca niezwłocznie poinformuje Zleceniodawcę o otrzymaniu informacji lub zawiadomienia od osoby, której dane dotyczą, od organu nadzorczego ds. ochrony danych, innego organu lub osoby trzeciej, jeżeli informacja ta pozostaje w bezpośrednim lub pośrednim związku z przetwarzaniem danych osobowych w ramach niniejszej umowy.

4.9 W związku ze zleconym przetwarzaniem danych Zleceniobiorca będzie wspierał Zleceniodawcę, w zakresie wymaganym przepisami prawa, przy tworzeniu i aktualizacji rejestru czynności przetwarzania, przy przeprowadzaniu oceny skutków dla ochrony danych oraz, w stosownych przypadkach, przy uprzednich konsultacjach z organem nadzorczym w rozumieniu art. 36 RODO, a także przekaże wszelkie niezbędne dane i informacje. Ponadto Zleceniobiorca będzie prowadził własny rejestr czynności przetwarzania oraz, jeżeli będzie to konieczne, przeprowadzi oceny skutków dla ochrony danych i powoła inspektora ochrony danych.

4.10 Zleceniobiorca ma obowiązek niezwłocznie, nie później jednak niż w ciągu 24 godzin, poinformować Zleceniodawcę, jeżeli przekazane mu dane osobowe zostały wykorzystane niezgodnie z prawem lub jeżeli osobom, których dane dotyczą, grozi szkoda. Przekazuje Zleceniodawcy wszelkie niezbędne informacje, aby ten mógł wypełnić swoje obowiązki informacyjne wobec osób, których dane dotyczą, zgodnie z przepisami o ochronie danych.

4.11 Każde przekazanie danych osobowych przez Zleceniobiorcę do państwa trzeciego lub organizacji międzynarodowej następuje zgodnie z prawem Unii lub prawem krajowym, a w szczególności musi być zgodne z postanowieniami RODO.

4.12 Strony mogą uzgodnić w Załączniku 2 dalsze klauzule dotyczące świadczenia usługi przetwarzania danych osobowych, o ile nie pozostają one w bezpośredniej ani pośredniej sprzeczności z niniejszą umową i nie naruszają praw ani wolności podstawowych osób, których dane dotyczą, ani ochrony przyznanej przez RODO.

4.13 Zleceniobiorca ma obowiązek niezwłocznie poinformować Zleceniodawcę, jeżeli jego zdaniem polecenie Zleceniodawcy narusza przepisy o ochronie danych obowiązujące w Unii lub w państwach członkowskich.

5. DALSZE PODMIOTY PRZETWARZAJĄCE

5.1 W zależności od uzgodnionego umownie zakresu usług do przetwarzania danych włączana jest określona lista dopuszczonych dalszych podmiotów przetwarzających.

5.2 Korzystanie z dalszych podmiotów przetwarzających może wiązać się z przekazywaniem danych do państw trzecich. Zleceniobiorca zapewnia, że przy przekazywaniu danych osobowych do państw trzecich spełnione są wymogi art. 44–49 RODO, oraz informuje Zleceniodawcę o zastosowanych zabezpieczeniach (na przykład standardowych klauzulach umownych, decyzji stwierdzającej odpowiedni stopień ochrony).

5.3 Lista dalszych podmiotów przetwarzających zatwierdzonych przez Zleceniodawcę przy zawarciu umowy znajduje się w Załączniku 3.

5.4 Między Zleceniobiorcą a dalszym podmiotem przetwarzającym musi zostać zawarta umowa zgodna z art. 28 ust. 4 RODO. Dalsze powierzenie musi uwzględniać przepisy o ochronie danych w takim samym zakresie, w jakim zostały one uzgodnione między Zleceniodawcą a Zleceniobiorcą w niniejszej umowie, a przetwarzanie danych może następować wyłącznie w celu wskazanym w odrębnie zleconej usłudze.

5.5 Zleceniobiorca ma obowiązek regularnie sprawdzać, czy dalsze podmioty przetwarzające przestrzegają obowiązków w zakresie ochrony danych wynikających z niniejszej umowy. Jeżeli w toku takiej kontroli Zleceniobiorca poweźmie wiadomość, że dalszy podmiot przetwarzający nie wypełnia lub wypełnia w niewystarczającym stopniu ciążące na nim obowiązki, ma obowiązek niezwłocznie i bez wezwania poinformować o tym Zleceniodawcę.

5.6 Dalsze powierzenie przetwarzania lub zmiana dotychczasowych dalszych podmiotów przetwarzających są dopuszczalne, o ile:

- Zleceniobiorca zapowie takie dalsze powierzenie z co najmniej dwutygodniowym wyprzedzeniem, w formie pisemnej lub dokumentowej, oraz
- Zleceniodawca nie zgłosi w formie pisemnej lub dokumentowej sprzeciwu wobec planowanego powierzenia lub zmiany w terminie dwóch tygodni od otrzymania zapowiedzi, a przy pierwszym przekazaniu danych Zleceniobiorcy najpóźniej do chwili tego przekazania. W przypadku sprzeciwu wobec planowanego włączenia lub zmiany dalszego podmiotu przetwarzającego nie może on zostać wykorzystany w tym zakresie do czasu osiągnięcia porozumienia. Za zmianę w rozumieniu niniejszego punktu uważa się także rozszerzenie zakresu wykorzystania już wskazanego dalszego podmiotu przetwarzającego, w szczególności dodanie kolejnego miejsca przetwarzania w państwie trzecim.

6. KONTROLA I ZGODNOŚĆ

6.1 Zleceniobiorca umożliwia Zleceniodawcy lub wskazanym przez niego przedstawicielom przeprowadzanie audytów i inspekcji w celu weryfikacji przestrzegania postanowień niniejszej umowy. Audyty takie należy przeprowadzać z odpowiednim wyprzedzeniem i nie mogą one w sposób nieuzasadniony zakłócać działalności Zleceniobiorcy. Zleceniodawca przyjmuje do wiadomości, że ewentualne inspekcje u dalszych podmiotów przetwarzających należy uzgadniać bezpośrednio z nimi, a Zleceniobiorca nie ma wpływu na stosowane przy tym zasady.

Koszty przeprowadzenia audytu ponosi Zleceniodawca, chyba że audyt wykaże poważne naruszenie niniejszej umowy przez Zleceniobiorcę.

6.2 Wszyscy audytorzy zewnętrzni podlegają umowie o zachowaniu poufności.

6.3 Zleceniobiorca udostępnia Zleceniodawcy wszelkie niezbędne informacje i współpracuje z nim w celu wykazania zgodności z RODO.

7. OKRES OBOWIĄZYWANIA I ZAKOŃCZENIE UMOWY

7.1 Niniejsza umowa powierzenia przetwarzania pozostaje w mocy przez czas trwania czynności przetwarzania danych i kończy się wraz z zakończeniem świadczenia usług lub w inny sposób uzgodniony przez strony.

7.2 W przypadku zakończenia niniejszej umowy (a także w każdym wcześniejszym momencie na odpowiednie żądanie Zleceniodawcy) Zleceniobiorca, według swobodnego wyboru Zleceniodawcy, albo samodzielnie zniszczy przetwarzane dane osobowe (wraz z ewentualnymi kopiami), albo przekaże je w całości Zleceniodawcy, o ile nie stoją temu na przeszkodzie ustawowe obowiązki przechowywania. Do czasu usunięcia lub zwrotu danych podmiot przetwarzający nadal zapewnia przestrzeganie wszystkich wymogów. Jeżeli Zleceniodawca nie wypowie się co do sposobu postępowania, Zleceniobiorca zniszczy dane po upływie 30 dni od zakończenia umowy, z zastrzeżeniem ustawowych obowiązków przechowywania.

7.3 Zleceniobiorca jest w równym stopniu zobowiązany doprowadzić do zniszczenia lub przekazania danych przez ewentualne dalsze podmioty przetwarzające.

8. POSTANOWIENIA KOŃCOWE

8.1 Zmiany i uzupełnienia niniejszej umowy oraz wszystkich jej części wymagają pisemnego porozumienia, które może zostać zawarte także w formie elektronicznej (dokumentowej), oraz wyraźnego wskazania, że stanowi ono zmianę lub uzupełnienie niniejszej umowy. Dotyczy to również rezygnacji z niniejszego wymogu formy.

Punkt 2.3 ogólnych warunków handlowych (zmiana w drodze domniemania zgody) nie ma zastosowania do niniejszej umowy ani jej załączników.

8.2 Niniejsza umowa podlega prawu obowiązującemu w Austrii i zgodnie z nim powinna być interpretowana. Sądem właściwym jest sąd w Wiedniu.

8.3 Jeżeli poszczególne postanowienia niniejszej umowy są lub staną się nieważne albo niewykonalne, pozostała część umowy pozostaje nienaruszona. Postanowienia takie uznaje się za zastąpione regulacjami ważnymi i wykonalnymi, które w możliwie najpełniejszy sposób realizują zamierzony przez strony cel gospodarczy.

Załączniki

Załącznik 1: Środki techniczne i organizacyjne (TOM)

Środki techniczne

Praca w centrum danych z certyfikatem ISO 27001

Aplikacja fonio działa w centrum danych z certyfikatem ISO 27001.

> Certyfikaty bezpieczeństwa wydawane przez podmioty zewnętrzne, takie jak ISO 27001, potwierdzają, że organizacja spełnia określony standard zarządzania bezpieczeństwem informacji. Stanowią ważny element budowania zaufania klientów i partnerów.

Bezpieczeństwo fizyczne i kontrola dostępu do pomieszczeń biurowych

Pomieszczenia biurowe są odpowiednio zabezpieczone przed nieuprawnionym wstępem, zamykane poza godzinami pracy, a goście mogą w nich przebywać wyłącznie w stałej asyście.

> Ochrona pomieszczeń biurowych przed nieuprawnionym wstępem oraz zapewnienie stałej asysty osobom z zewnątrz przyczyniają się do ochrony danych osobowych przetwarzanych w biurze.

Ścisłe rozdzielenie środowisk produkcyjnych i testowych

Środowiska produkcyjne i testowe są ściśle rozdzielone zarówno logicznie, jak i infrastrukturalnie. Przetwarzanie rzeczywistych danych produkcyjnych (prawdziwych danych osobowych) w środowiskach testowych jest surowo zabronione. Jeżeli dane są potrzebne do celów testowych, muszą zostać w pełni zanonimizowane albo należy użyć danych syntetycznych.

> Środowiska produkcyjne i testowe są ściśle rozdzielone zarówno logicznie, jak i infrastrukturalnie.

Zapory sieciowe (firewalle)

Zapory sieciowe monitorują i kontrolują ruch przychodzący oraz wychodzący, dopuszczając wyłącznie niezbędne, jawnie autoryzowane połączenia.

> Zapory sieciowe to systemy bezpieczeństwa, które monitorują i sterują ruchem sieciowym na podstawie zdefiniowanych wcześniej reguł bezpieczeństwa. Tworzą barierę między zaufanymi wewnętrznymi segmentami sieci a niezaufanymi sieciami zewnętrznymi, takimi jak internet.

Protokoły i konfiguracje sieciowe zgodne ze stanem techniki

Bezpieczne, zgodne ze stanem techniki protokoły i konfiguracje sieciowe stosowane są jako środki hartowania, aby chronić dane w trakcie przesyłania.

> Bezpieczne protokoły sieciowe, na przykład poprawnie skonfigurowany HTTPS oparty na TLS, przyczyniają się do ochrony danych w trakcie przesyłania (data in transit).

Monitorowanie sieci

Aktywność sieciowa jest stale monitorowana w celu wykrywania zagrożeń bezpieczeństwa i reagowania na nie.

> Monitorowanie sieci to krytyczny proces IT, w ramach którego wszystkie komponenty sieciowe, takie jak routery, przełączniki, zapory, serwery i maszyny wirtualne, są stale nadzorowane i analizowane pod kątem błędów, incydentów bezpieczeństwa i problemów wydajnościowych, aby utrzymać i optymalizować dostępność systemów. Wczesne wykrycie problemów lub incydentów pozwala zapobiec nieoczekiwanym przestojom.

Hartowanie systemów

Środki hartowania wdrażane są we wszystkich istotnych systemach poprzez bezpieczną konfigurację opartą na benchmarkach CIS lub zaleceniach dostawcy.

> Bezpieczna konfiguracja systemu oznacza takie ustawienie systemów i oprogramowania, które zmniejsza ryzyko ich wykorzystania przez złośliwe podmioty. Obejmuje to działania takie jak wyłączanie zbędnych usług, ustawianie

odpowiednich uprawnień użytkowników oraz regularne aktualizowanie systemów.

Ochrona przed złośliwym oprogramowaniem

Wdrożono środki ochrony przed złośliwym oprogramowaniem, aby chronić systemy i dane. Obejmuje to instalację i utrzymanie oprogramowania wykrywającego złośliwe oprogramowanie w istotnych systemach oraz monitorowanie i obsługę alertów wywoływanych przez potencjalnie wykryte zagrożenia.

Środki ochrony przed złośliwym oprogramowaniem obejmują wykorzystanie narzędzi programowych do wykrywania i usuwania oprogramowania, które mogłoby zagrozić bezpieczeństwu systemu i integralności danych.

Proces zarządzania poprawkami

Wszystkie komponenty programowe i sprzętowe są regularnie aktualizowane w ramach dedykowanego procesu zarządzania poprawkami, aby chronić je przed znanymi podatnościami. Poprawki wgrywane są w różnych odstępach w zależności od typu systemu, jednak nie rzadziej niż raz na kwartał, a niezwłocznie wtedy, gdy poprawka usuwa krytyczną podatność.

Regularne aktualizacje oprogramowania i sprzętu zapewniają ochronę przed znanymi podatnościami. Aktualizacje często zawierają poprawki luk bezpieczeństwa wykrytych od czasu poprzedniej wersji oprogramowania lub sprzętu.

Zarządzanie tożsamością i dostępem (IAM) oraz procesy cyklu życia

Wdrożono scentralizowany system zarządzania tożsamością i dostępem (IAM) wraz z ustrukturyzowanym procesem „Joiner-Mover-Leaver” (JML).

Zintegrowany proces IAM i JML zapewnia, że tożsamości użytkowników, prawa dostępu i uprawnienia są systematycznie zarządzane przez cały cykl zatrudnienia: od wdrożenia (joiner), przez wewnętrzne zmiany ról (mover), aż po zakończenie współpracy (leaver). Wraz z zakończeniem stosunku pracy lub umowy wszystkie uprawnienia dostępu do danych osobowych i systemów wewnętrznych są automatycznie i niezwłocznie odbierane. Skutecznie ogranicza to ryzyko tak zwanego privilege creep, czyli pełzającego rozszerzania uprawnień, i zapobiega nieuprawnionemu dostępowi przez byłych pracowników lub zewnętrznych usługodawców.

Koncepcja uprawnień

Wdrożono ścisłe kontrole dostępu do danych osobowych oparte na zasadach „need-to-know” (wiedza wyłącznie w razie potrzeby) i „least privilege” (minimalne uprawnienia). Tam, gdzie jest to możliwe i zasadne, stosowane jest uwierzytelnianie wieloskładnikowe (MFA), a także wymagane jest obowiązkowe korzystanie z menedżerów haseł oraz stosowanie haseł generowanych losowo o długości co najmniej 20 znaków. Uprawnienia administracyjne przyznawane są zgodnie z zasadą dwóch par oczu i mogą być wykorzystywane wyłącznie w uzasadnionych celach. Korzystanie z uprawnień administracyjnych jest monitorowane.

Kontrole dostępu to środki określające, kto może uzyskać dostęp do określonych zasobów, takich jak dane osobowe. Mają kluczowe znaczenie dla zapobiegania nieuprawnionemu dostępowi i zapewnienia, że do danych sięgają wyłącznie osoby upoważnione.

Ograniczenie czynności administracyjnych do wykwalifikowanego personelu

Czynności administracyjne na komponentach infrastruktury może wykonywać wyłącznie specjalnie przeszkolony, wykwalifikowany i upoważniony personel. Upoważnienie przyznawane jest ściśle na podstawie wykazanych kompetencji zawodowych, a użytkownicy administracyjni są zobowiązani do odbywania regularnych, udokumentowanych szkoleń dotyczących bezpieczeństwa w zakresie czynności administracyjnych.

Ograniczenie dostępu administracyjnego do zweryfikowanych specjalistów zapewnia, że krytyczne zmiany w systemach wykonują wyłącznie kompetentne osoby. Minimalizuje to ryzyko luk bezpieczeństwa, błędnych konfiguracji lub przypadkowej utraty danych wskutek błędu ludzkiego albo braku wiedzy technicznej.

Zarządzanie sesjami i automatyczne wygasanie

Sesje użytkowników i administratorów w aplikacjach oraz wewnętrznych systemach administracyjnych są automatycznie kończone po upływie zdefiniowanego czasu bezczynności.

Automatyczne wygasanie sesji ogranicza ryzyko nieuprawnionego dostępu do danych w sytuacji, gdy stanowisko pracy lub urządzenie mobilne pozostaje bez nadzoru w niezabezpieczonym otoczeniu.

Postępowanie z danymi logowania i innymi informacjami wrażliwymi

Do zabezpieczenia dostępu do danych osobowych stosowane jest uwierzytelnianie dwuskładnikowe (2FA). Dane logowania i inne informacje wrażliwe przechowywane są w menedżerze haseł. Wszystkie punkty dostępu do menedżera haseł są szyfrowane.

Uwierzytelnianie dwuskładnikowe stanowi dodatkową warstwę zabezpieczeń, ponieważ użytkownik musi przedstawić dwa dowody tożsamości, zanim uzyska dostęp do danych. Znacznie utrudnia to osobom nieuprawnionym uzyskanie dostępu do danych i systemów.

Narzędzia do zarządzania hasłami

Narzędzia do zarządzania hasłami służą do tworzenia, przechowywania i zarządzania bezpiecznymi hasłami do systemów i aplikacji, zgodnie z wewnętrzną polityką haseł.

Narzędzia do zarządzania hasłami pomagają użytkownikom generować, przechowywać i zarządzać unikalnymi, złożonymi hasłami do różnych kont, co zmniejsza ryzyko ponownego wykorzystania haseł i poprawia ogólne bezpieczeństwo.

Szyfrowanie danych

Dane przechowywane (data at rest) oraz dane przesyłane (data in transit) są szyfrowane zgodnie ze sprawdzonymi praktykami branżowymi, aby chronić je przed nieuprawnionym dostępem.

Szyfrowanie danych zapewnia, że dane wrażliwe są przechowywane i przesyłane w postaci nieczytelnej, co chroni je przed nieuprawnionym dostępem, w szczególności w razie kradzieży lub utraty nośnika.

Pseudonimizacja danych

Stosowane są techniki pseudonimizacji danych osobowych, aby zmniejszyć ryzyko naruszeń ochrony danych.

Pseudonimizacja to metoda deidentyfikacji, w której pola identyfikujące osobę w zbiorze danych zastępowane są jednym lub kilkoma sztucznymi identyfikatorami albo pseudonimami.

Rejestrowanie zdarzeń (logi audytowe)

Prowadzone są logi audytowe, aby rejestrować, kto i kiedy uzyskał dostęp do których danych osobowych. Ponadto logi istotne dla bezpieczeństwa są przechowywane w postaci niemodyfikowalnej.

Logi audytowe rejestrują momenty, w których użytkownicy uzyskują dostęp do systemów i danych. Może to mieć kluczowe znaczenie w razie incydentu bezpieczeństwa, ponieważ pomaga odtworzyć przebieg zdarzeń i zidentyfikować potencjalnych sprawców.

Regularne kopie zapasowe

Dane są regularnie kopiowane wszędzie tam, gdzie jest to niezbędne i uzasadnione, aby zapobiec ich utracie.

Regularne kopie zapasowe mają kluczowe znaczenie dla zapobiegania utracie danych w razie incydentów, takich jak naruszenia ochrony danych czy awarie techniczne. Zapewniają, że nawet w najgorszym przypadku organizacja może odtworzyć dane i utrzymać ciągłość działania.

Automatyczne skanowanie podatności

Automatyczne wewnętrzne i zewnętrzne skanowanie podatności prowadzone jest regularnie we wszystkich komponentach infrastruktury, aplikacjach i segmentach sieci.

Automatyczne skanowanie uzupełnia regularne testy penetracyjne, wykrywając w czasie rzeczywistym nowo ujawnione luki bezpieczeństwa i błędne konfiguracje, co umożliwia szybkie usunięcie ich poprawkami.

Testy penetracyjne

Regularnie przeprowadzane są testy penetracyjne w celu identyfikacji potencjalnych podatności w systemach.

Testy penetracyjne, zwane też pentestami, to symulowane cyberataki na systemy informatyczne i środowiska IT, mające ujawnić możliwe do wykorzystania podatności. Proces obejmuje zebranie informacji o celu przed testem, identyfikację potencjalnych punktów wejścia, próbę ich przełamania oraz zaraportowanie wyników.

Środki organizacyjne

Polityki bezpieczeństwa informacji

Polityki bezpieczeństwa informacji zostały wdrożone oraz są regularnie przeglądane i aktualizowane.

Polityki bezpieczeństwa informacji tworzą ramy tego, czego oczekuje się od pracowników i systemów w zakresie bezpieczeństwa informacji. Regularny przegląd i aktualizacja tych polityk zapewniają, że pozostają one skuteczne i aktualne wobec zmieniającego się krajobrazu zagrożeń.

Inspektor ochrony danych (IOD)

Powołano inspektora ochrony danych (IOD), który nadzoruje zgodność z RODO.

Inspektor ochrony danych odpowiada za nadzór nad strategią ochrony danych w przedsiębiorstwie oraz jej wdrożeniem, aby zapewnić zgodność z wymogami RODO. IOD pełni funkcję punktu kontaktowego dla przedsiębiorstwa, osób, których dane dotyczą, oraz organów nadzorczych.

Ochrona danych w fazie projektowania i domyślna ochrona danych (privacy by design i privacy by default)

Przestrzegane są zasady ochrony danych w fazie projektowania (privacy by design) oraz domyślnej ochrony danych (privacy by default).

Zasady te dotyczą wbudowania ochrony danych w czynności przetwarzania i praktyki biznesowe, od fazy rozwoju przez cały cykl życia. Dzięki temu ochrona danych nie jest refleksją po fakcie, lecz jest trwale osadzona w projekcie i architekturze systemów IT oraz praktyk biznesowych.

Zasada minimalizacji danych

Przestrzegana jest zasada minimalizacji danych; zbierane są wyłącznie dane osobowe niezbędne do świadczenia usługi.

Minimalizacja danych to jedna z podstawowych zasad RODO. Oznacza, że organizacja powinna zbierać i przetwarzać wyłącznie te dane osobowe, których potrzebuje do swojego określonego celu.

Rejestr czynności przetwarzania (RCP)

Prowadzimy zgodny z RODO rejestr czynności przetwarzania, dokumentujący wszystkie istotne operacje przetwarzania, powiązane przepływy danych, zaangażowane podmioty trzecie oraz podstawę prawną każdej czynności.

Rejestr czynności przetwarzania zapewnia przejrzystość przepływów danych i pomaga identyfikować potencjalne ryzyka związane z przetwarzaniem. Ponadto zapewnia, że każda czynność przetwarzania i każde przekazanie danych osobowych opiera się na ważnej podstawie prawnej.

Oceny skutków dla ochrony danych (DPIA) i oceny skutków transferu (TIA)

Regularnie przeprowadzane są oceny skutków dla ochrony danych oraz oceny skutków transferu (TIA), aby identyfikować i ograniczać ryzyka zarówno przy przetwarzaniu, jak i przy przekazywaniu danych osobowych poza granice przedsiębiorstwa i kraju.

Oceny skutków dla ochrony danych (DPIA) oraz oceny skutków transferu (TIA) identyfikują, oceniają i ograniczają lub minimalizują ryzyka związane z ochroną danych przy ich przetwarzaniu. Są istotne, ponieważ pomagają organizacjom wcześnie rozpoznać i usunąć problemy, ograniczając związane z nimi koszty oraz potencjalne szkody wizerunkowe.

Zarządzanie ryzykiem dostawców i umowy powierzenia (AVV)

Przeprowadzane są weryfikacje bezpieczeństwa informacji u podmiotów przetwarzających oraz zawierane są umowy powierzenia przetwarzania (AVV), aby zapewnić i umownie zabezpieczyć przestrzeganie standardów

bezpieczeństwa.

Weryfikacje bezpieczeństwa informacji u podmiotów przetwarzających mają kluczowe znaczenie dla sprawdzenia, czy zewnętrzni usługodawcy lub dostawcy przestrzegają tych samych standardów ochrony danych i bezpieczeństwa co własna organizacja. Pomaga to minimalizować ryzyko naruszeń lub wycieków danych za pośrednictwem podmiotów trzecich. Zgodnie z RODO musi to zostać formalnie uregulowane umową powierzenia przetwarzania (AVV).

Procedura obsługi praw osób, których dane dotyczą

Wdrożono standardowy przepływ pracy zapewniający, że wnioski osób, których dane dotyczą, takie jak prawo dostępu, sprostowania czy przenoszenia danych, są weryfikowane, rozpatrywane i realizowane w terminach ustawowych.

Ustanowienie jasnej procedury wewnętrznej dla praw osób, których dane dotyczą, zapewnia zgodność z obowiązkami informacyjnymi wynikającymi z RODO oraz zapobiega eskalacjom prawnym i skargom do organów nadzorczych.

Szkolenia pracowników

Pracownicy przechodzą regularne szkolenia z zakresu ochrony danych i zgodności z RODO.

Regularne szkolenia zapewniają, że pracownicy znają zasady ochrony danych oraz swoje obowiązki wynikające z RODO. Może to pomóc zapobiegać naruszeniom ochrony danych spowodowanym błędem ludzkim oraz zapewnić prawidłowe zgłaszanie i rozwiązywanie problemów.

Kampanie budowania świadomości bezpieczeństwa informacji

Regularnie prowadzone są kampanie i szkolenia budujące świadomość użytkowników w zakresie bezpieczeństwa informacji, aby uświadamiać pracownikom potencjalne cyberzagrożenia.

Kampanie budowania świadomości bezpieczeństwa informacji mają kluczowe znaczenie dla uświadamiania pracownikom zagrożeń takich jak phishing, socjotechnika czy złośliwe oprogramowanie oraz dla promowania dobrych praktyk w zakresie ochrony danych.

Szkolenia z bezpiecznego programowania dla deweloperów

Programistom regularnie oferowane są szkolenia z bezpieczeństwa, aby zapewnić stosowanie bezpiecznych praktyk programistycznych.

Regularne szkolenia z bezpieczeństwa dla programistów są niezbędne, aby zwiększać świadomość najnowszych zagrożeń i dobrych praktyk bezpiecznego wytwarzania oprogramowania, a tym samym zmniejszać prawdopodobieństwo przedostania się podatności do oprogramowania.

Procedura usuwania danych (retencja i usuwanie)

Na podstawie koncepcji usuwania danych dane osobowe są automatycznie usuwane, o ile pozwala na to prawo, gdy tylko cel świadczenia usługi został osiągnięty albo gdy osoba, której dane dotyczą, wyraźnie tego zażąda (prawo do usunięcia danych, prawo do bycia zapomnianym).

Regularne usuwanie danych, które nie służą już żadnemu celowi, jest ważnym elementem zarządzania danymi i zgodności z RODO. Pomaga zmniejszyć ryzyko naruszeń ochrony danych i zapewnia, że organizacja nie przechowuje danych osobowych dłużej, niż jest to konieczne.

Plan reagowania na incydenty bezpieczeństwa

Opracowano szczegółowy plan reagowania na potencjalne naruszenia ochrony danych lub incydenty cyberbezpieczeństwa dotyczące danych osobowych.

Plan reagowania na incydenty to zbiór instrukcji pomagających identyfikować incydenty bezpieczeństwa, reagować na nie i przywracać stan normalny. Solidny plan ma kluczowe znaczenie dla minimalizowania skutków naruszenia i umożliwienia szybkiego przywrócenia działania.

Procedura zgłaszania naruszeń ochrony danych

Wdrożono procedurę zgłaszania naruszeń ochrony danych, aby informować osoby, których dane dotyczą, organy nadzorcze oraz inne właściwe podmioty.

W razie naruszenia ochrony danych RODO zobowiązuje organizacje do powiadomienia osób, których dane dotyczą, oraz właściwych organów nadzorczych. Procedura ta umożliwia terminowe powiadomienie i może pomóc złagodzić skutki naruszenia.

Regularny przegląd praktyk ochrony danych

Praktyki zarządzania ochroną danych są przeglądane w regularnych odstępach, aby zapewnić ich aktualność i prawidłowe wdrożenie, a ewentualne odchylenia są oceniane i usuwane.

Regularne przeglądy praktyk ochrony danych zapewniają, że zmiany w przetwarzaniu lub luki w środkach są identyfikowane i odpowiednio adresowane, aby unikać odchyleń od wymogów RODO albo wcześnie je wykrywać i usuwać.

Załącznik 2: Postanowienia uzupełniające

Dane osobowe nie są wykorzystywane do trenowania, ulepszania ani ewaluacji modeli AI, ani przez Zleceniobiorcę, ani przez jego dalsze podmioty przetwarzające.

Jeżeli niniejsza umowa powierzenia zawierana jest z partnerem resellerskim, fonio przyjmuje wobec tego partnera rolę dalszego podmiotu przetwarzającego.

Stosowane są następujące standardowe terminy usuwania danych:

Kategoria danych	Termin usunięcia
Nagrania audio	30 dni od zakończenia połączenia
Transkrypcje przebiegu rozmowy	90 dni od zakończenia połączenia
Logi dialogów i protokoły techniczne	30 dni od zakończenia połączenia
Metadane telefoniczne	6 miesięcy od zakończenia połączenia
Dokumenty istotne księgowo	7 lat, ustawowy okres przechowywania od wystawienia

Dla ewentualnych innych kategorii danych obowiązuje punkt 7.2 niniejszej AVV.

Załącznik 3: Dalsze podmioty przetwarzające

Dostawcy główni świadczenia usługi

Poniżsi dostawcy są wykorzystywani zawsze. W przypadku gdy na wyraźne życzenie klienta jako dostawca główny wybrany został dostawca zapasowy, istnieje możliwość, również na wyraźne życzenie klienta, rezygnacji z dotychczasowego dostawcy z poniższej listy dostawców głównych.

Hetzner Online GmbH

Adres	Industriestr. 25, 91710 Gunzenhausen, Niemcy
Usługa	Hosting systemu
Podstawa transferu	Brak przekazywania do państwa trzeciego.
Lokalizacja serwerów	Wykorzystywane są centra danych w Norymberdze, Falkenstein i Helsinkach. Więcej informacji: https://docs.hetzner.com/cloud/general/locations/
Przechowywanie danych	Atest BSI C5:2020 z 02.03.2026: https://files.hetzner.com/docs/BSI-C52020Typ2_Testat_2026.pdf

Twilio Ireland Limited

Adres	25-28 North Wall Quay, D01 H104 Dublin, Irlandia
Usługa	Telefonia
Podstawa transferu	EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/list). Swiss-U.S. Data Privacy Framework (https://www.dataprivacyframework.gov/list). Wiążące reguły korporacyjne uzgodniono jako pomocnicze umowne zabezpieczenie (fallback) dla międzynarodowego transferu danych: https://www.twilio.com/en-us/legal/bcr/processor. Dodatkowo umownie uzgodniono standardowe klauzule umowne (moduł 3) wraz ze „Swiss Finish", aby zapewnić pełną ochronę danych osobowych przy transferach międzynarodowych.
Lokalizacja serwerów	UE, region Irlandia. Więcej informacji: https://www.twilio.com/docs/global-infrastructure/edge-locations
Przechowywanie danych	Dane audio nie są przechowywane (Zero Data Retention).

LiveKit Inc.

Adres	4285 Payne Avenue, Suite 9154, CA 95157 San Jose, Kalifornia, Stany Zjednoczone
Usługa	Wirtualne pokoje rozmów
Podstawa transferu	EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/list). Swiss-U.S. Data Privacy Framework (https://www.dataprivacyframework.gov/list). Standardowe klauzule umowne (moduł 3) wraz ze „Swiss Finish" uzgodniono jako pomocnicze umowne zabezpieczenie (fallback) dla międzynarodowego transferu danych.
Lokalizacja serwerów	Dzięki konfiguracji region pinning dane nie opuszczają regionu europejskiego. Więcej informacji: https://docs.livekit.io/deploy/admin/regions/region-pinning/
Przechowywanie danych	Dane audio nie są trwale przechowywane (streaming w czasie rzeczywistym / ZDR).

Soniox, Inc.

Adres	1045 Helm Ln, Foster City, CA 94404, Stany Zjednoczone
Usługa	Rozpoznawanie mowy (speech-to-text)
Podstawa transferu	Standardowe klauzule umowne (moduł 3), ustalone umownie w AVV zawartej z Soniox.
Lokalizacja serwerów	Przetwarzanie w Europie w ramach umowy enterprise. Więcej informacji: https://soniox.com/europe
Przechowywanie danych	Dane audio nie są przechowywane (Zero Data Retention).

OpenAI Ireland Ltd.

Adres	1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Irlandia
Usługa	Model językowy (LLM)
Podstawa transferu	Standardowe klauzule umowne UE (SCC, moduł 3) wraz ze „Swiss Finish", ustalone umownie w AVV zawartej z OpenAI.
Lokalizacja serwerów	Przetwarzanie w Europie w ramach umowy enterprise. Więcej informacji: https://openai.com/index/introducing-data-residency-in-europe/
Przechowywanie danych	Stosowane jest Zero Data Retention.

Theai, Inc. dba Inworld AI

Adres	1975 W El Camino Real #300, Mountain View, CA 94040, Stany Zjednoczone
Usługa	Synteza mowy (text-to-speech)
Podstawa transferu	Standardowe klauzule umowne (moduł 3) uzgodnione dla międzynarodowego transferu danych.
Lokalizacja serwerów	Rezydencja danych w UE uzgodniona w umowie enterprise.
Przechowywanie danych	Dane audio nie są przechowywane (Zero Data Retention). Więcej informacji: https://docs.inworld.ai/portal/zero-data-retention. Informacje o bezpieczeństwie i certyfikatach: https://trust.inworld.ai/

Sinch AB (Mailgun)

Adres	Lindhagensgatan 112, 112 51 Sztokholm, Szwecja
Usługa	Wysyłka poczty elektronicznej
Podstawa transferu	Umowę powierzenia zawarto ze spółką Sinch AB w Sztokholmie, będącą spółką matką amerykańskiego przedsiębiorstwa Mailgun Technologies, Inc., 112 E Pecan St #113, San Antonio, TX 78205, Stany Zjednoczone. Mailgun Technologies, Inc. jest uczestnikiem EU-US Data Privacy Framework: https://sinch.com/legal/terms-and-conditions/other-sinch-terms-conditions/data-processing-agreement/. Standardowe klauzule umowne (moduł 3) uzgodniono jako pomocnicze umowne zabezpieczenie (fallback) dla międzynarodowego transferu danych.
Lokalizacja serwerów	Region „EU”. Więcej informacji: https://www.mailgun.com/about/regions/

New Relic, Inc.

Adres	188 Spear Street, Suite 1200, CA 94105 San Francisco, Kalifornia, Stany Zjednoczone
Usługa	Rejestrowanie zdarzeń i monitoring
Podstawa transferu	EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/list). Swiss-U.S. Data Privacy Framework (https://www.dataprivacyframework.gov/list). Standardowe klauzule umowne (moduł 3) wraz ze „Swiss Finish” uzgodniono jako pomocnicze umowne zabezpieczenie (fallback) dla międzynarodowego transferu danych.
Lokalizacja serwerów	fonio korzysta z lokalizacji europejskiej. Więcej informacji: https://docs.newrelic.com/docs/accounts/accounts-billing/account-setup/choose-your-data-center/

Dostawcy zapasowi zwiększający dostępność

Poniżsi dostawcy pełnią rolę zapasową na wypadek awarii dostawcy głównego lub niemożności zapewnienia przez niego wymaganej jakości usługi. Służy to zwiększeniu dostępności i jakości usługi. Dostawcy zapasowi są domyślnie włączeni, lecz mogą zostać wyłączeni na życzenie klienta. Na wyraźne życzenie klienta wymienieni dostawcy mogą być również wykorzystywani jako dostawcy główni.

Deepgram, Inc.

Adres	548 Market St, Suite 25104, CA 94104-5401 San Francisco, Kalifornia, Stany Zjednoczone
Usługa	Rozpoznawanie mowy (speech-to-text)
Podstawa transferu	Standardowe klauzule umowne UE (SCC, moduł 3), ustalone umownie w AVV zawartej z Deepgram.
Lokalizacja serwerów	Przetwarzanie wyłącznie w Europie, poprzez własny punkt końcowy UE, w ramach umowy enterprise.
Przechowywanie danych	Dane audio nie są przechowywane (Zero Data Retention).

Google Ireland Limited

Adres	Gordon House, Barrow Street, Dublin 4, D04 E5W5, Irlandia
Usługa	Model językowy (LLM)
Podstawa transferu	EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/list). Swiss-U.S. Data Privacy Framework (https://www.dataprivacyframework.gov/list). Standardowe klauzule umowne (moduł 3) wraz ze „Swiss Finish” uzgodniono jako pomocnicze umowne zabezpieczenie (fallback) dla międzynarodowego transferu danych.
Lokalizacja serwerów	Region europejski.
Przechowywanie danych	Dane audio nie są przechowywane (Zero Data Retention).

Eleven Labs Inc.

Adres	169 Madison Ave #2484, NY 10016 Nowy Jork, Nowy Jork, Stany Zjednoczone
Usługa	Synteza mowy (text-to-speech)
Podstawa transferu	EU-US Data Privacy Framework (https://elevenlabs.io/privacy-policy). Standardowe klauzule umowne (moduł 3) uzgodniono jako pomocnicze umowne zabezpieczenie (fallback) dla międzynarodowego transferu danych.
Lokalizacja serwerów	W ramach umowy enterprise wszystkie dane pozostają wyłącznie na terenie Europy. Więcej informacji: https://elevenlabs.io/docs/overview/administration/data-residency
Przechowywanie danych	Dane audio nie są przechowywane (Zero Data Retention).

Dostawcy opcjonalni

Poniżsi dostawcy wykorzystywani są opcjonalnie i wyłącznie na wyraźne życzenie klienta.

Nylas, Inc.

Adres	2100 Geng Rd. #2100, Palo Alto, CA 94303, Stany Zjednoczone
Usługa	Integracja kalendarza: podłączenie kont kalendarzowych (Google Calendar, Microsoft Outlook) przez OAuth w celu sprawdzania dostępności, rezerwacji spotkań i dwukierunkowej synchronizacji wydarzeń.
Podstawa transferu	EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/list). Swiss-U.S. Data Privacy Framework (https://www.dataprivacyframework.gov/list). Standardowe klauzule umowne (moduł 3) uzgodniono jako pomocnicze umowne zabezpieczenie (fallback) dla międzynarodowego transferu danych.
Lokalizacja serwerów	Regionem rezydencji danych jest Europa (Irlandia). Więcej informacji: https://developer.nylas.com/docs/dev-guide/platform/data-residency/

Meta Platforms Ireland Ltd.

Adres	Merrion Road, Dublin 4, D04 X2K5, Irlandia
Usługa	Integracja z WhatsApp
Podstawa transferu	EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/list). Swiss-U.S. Data Privacy Framework (https://www.dataprivacyframework.gov/list). Standardowe klauzule umowne (moduł 3) uzgodniono jako pomocnicze umowne zabezpieczenie (fallback) dla międzynarodowego transferu danych.

SideGuide Technologies, Inc. (Firecrawl)

Adres	2261 Market Street STE 85367, CA 94114 San Francisco, Stany Zjednoczone
Usługa	Wyszukiwarka
Podstawa transferu	Standardowe klauzule umowne (moduł 3) wraz ze „Swiss Finish”.

LangChain, Inc.

Adres	501 2nd Street, Suite 120, CA 94107 San Francisco, Stany Zjednoczone
Usługa	Integracja czatu
Podstawa transferu	Standardowe klauzule umowne (moduł 3).

Uzupełnienia dotyczące mechanizmów failover

Aby zapewnić dostępność naszej usługi i jej jakość, w przypadku niedostępności lub niewystarczającej dostępności lokalizacji w UE, i wyłącznie w takim przypadku, stosujemy dla poniższych dostawców failover do Stanów Zjednoczonych, czyli tymczasowe przekierowanie przepływu danych danego dostawcy na lokalizacje serwerowe w USA:

- Soniox, Inc.
- OpenAI Ireland Ltd.
- Theai, Inc. dba Inworld AI

Mechanizmy failover stosowane są wyłącznie przez minimalny niezbędny czas. Wyłączenie failovera do Stanów Zjednoczonych jest możliwe w każdej chwili na życzenie klienta.

Załącznik 4: Oświadczenie o zachowaniu poufności i ochronie danych

Do niniejszej umowy jako Załącznik 4 dołączone zostają poniższe oświadczenia o zachowaniu poufności. Zleceniodawca może skorzystać z właściwej dla siebie wersji bez zmian jej treści:

- Oświadczenie o zachowaniu poufności i ochronie danych — Niemcy (§§ 203, 204 StGB, § 62a StBerG, § 43e BRAO);
- Oświadczenie o zachowaniu poufności i ochronie danych — Austria (§ 121 StGB, § 54 ÄrzteG, § 9 RAO, § 80 WTBG 2017, § 6 DSG).