

POLITYKA PRYWATNOŚCI APLIKACJI ANDROID „SIDEKICK AI MANAGER ASSISTANT”

Wersja: 2.0

Data wejścia w życie: 23.07.2026

§ 1. ADMINISTRATOR

Administratorem danych osobowych jest:

Łukasz Gnoiński

Leszczynowa 42

05-090 Laszczki Polska

support@sidekickai.app

Kontakt w sprawach ochrony danych: support@sidekickai.app

§ 2. ZAKRES POLITYKI I ROLA PODMIOTÓW

1. Polityka opisuje przetwarzanie danych związane z Aplikacją.
2. Aplikacja jest przeznaczona przede wszystkim dla managera lub osoby zarządzającej zespołem.
3. Pracownicy i inne osoby, których dane są wprowadzane do Aplikacji lub których głos jest nagrywany, mogą być osobami trzecimi i nie muszą być użytkownikami Aplikacji.
4. W zależności od konkretnego modelu korzystania z Aplikacji i relacji prawnych, Użytkownik może samodzielnie ustalać cele i sposoby przetwarzania danych osób trzecich. W takim zakresie może być odrębnym administratorem danych.
5. Operator nie może samą Polityką przesądzić o roli prawnej stron. Role Administratora, podmiotu przetwarzającego lub innych podmiotów należy oceniać zgodnie z faktycznym sposobem przetwarzania.
6. Użytkownik pozostaje odpowiedzialny za legalność danych, których przetwarzanie sam inicjuje, w zakresie wynikającym z jego własnych działań i obowiązków.

§ 3. KATEGORIE DANYCH

Na urządzeniu mogą być przechowywane:

1. dane profili osób: imię, nazwisko, opcjonalnie e-mail, telefon, kolor i status;
2. metadane nagrań: data, czas trwania i ścieżka pliku;
3. pliki audio rozmów i notatek głosowych;
4. transkrypcje, źródło transkrypcji, podsumowania AI i wykryte zadania;
5. notatki tekstowe i oznaczenia dodane przez Użytkownika;
6. zadania, terminy, statusy i powiązane osoby;

7. dane urlopów i nieobecności;
8. próbka głosu managera wykorzystywana do rozpoznawania mówcy;
9. maksymalnie 50 najczęstszych wyuczonych słów lub fraz;
10. dane techniczne i rozliczeniowe opisane w dalszych paragrafach.

Aplikacja nie otrzymuje ani nie przechowuje samego PIN-u, wzoru ani danych biometrycznych obsługiwanych przez system Android.

§ 4. RETENCJA

1. Surowe nagranie audio i surowa transkrypcja są automatycznie usuwane po 7 dniach zgodnie z działaniem Aplikacji.
2. Treść może zostać zachowana w postaci trwałej notatki tekstowej, jeżeli dana funkcja tak działa.
3. Cotygodniowe podsumowania AI są przechowywane około 6 miesięcy, a następnie automatycznie usuwane.
4. Notatki, zadania, profile i dane urlopów są przechowywane do czasu ich usunięcia przez Użytkownika albo do czasu usunięcia zgodnie z działaniem Aplikacji lub obowiązkiem prawnym.
5. Lista wyuczonych słów jest ograniczona do maksymalnie 50 najczęstszych elementów.
6. Retencja u dostawców zewnętrznych może wynikać również z ich aktualnych warunków, umów, konfiguracji usługi i obowiązków prawnych.

§ 5. PRZETWARZANIE LOKALNE – PLAN FREE

1. W planie Free transkrypcja audio–tekst wykonywana jest lokalnie na urządzeniu przy użyciu modelu Parakeet TDT.
2. W tym trybie nagranie ani transkrypt nie są wysyłane poza urządzenie w celu transkrypcji.
3. Wykrywanie zadań działa lokalnie bez wysyłania treści do chmury AI.

§ 6. CHMURA AI – PLAN PREMIUM/PRO

1. Po włączeniu funkcji chmury AI plik audio może zostać przesłany do ElevenLabs w celu transkrypcji.
2. Wraz z audio może być przesłane imię i nazwisko pracownika jako keyterm wspierający rozpoznawanie poprawnej pisowni.
3. Przy korzystaniu z proxy Aplikacji żądanie przechodzi przez backend hostowany w Google Cloud Run.
4. Zgodnie z aktualnym działaniem backend nie zapisuje trwale treści audio ani transkryptów przechodzących przez proxy.

5. W planie Pro Użytkownik może, jeśli funkcja jest dostępna, użyć własnego klucza API i przesłać dane bezpośrednio do dostawcy.

6. Przy podsumowaniach i wnioskach AI do Mistral AI lub Google Gemini może trafić pełny tekst transkrypcji, oznaczenia mówców, kontekst historyczny dotyczący pracownika, podsumowania, zadania, terminy, kontekst zespołu i pytanie Użytkownika – w zakresie zależnym od konkretnej funkcji.

7. Dostawca AI może być wybierany automatycznie przez Aplikację.

§ 6a. ODPOWIEDZIALNOŚĆ ZA KORZYSTANIE Z FUNKCJI NAGRYWANIA I AI

1. Operator udostępnia wyłącznie narzędzie techniczne umożliwiające nagrywanie rozmów, wykonywanie transkrypcji oraz korzystanie z funkcji AI.

2. Operator nie weryfikuje, czy Użytkownik posiada podstawę prawną do nagrywania rozmów lub przetwarzania danych osób trzecich.

3. Korzystając z funkcji nagrywania i AI Użytkownik odpowiada za zgodność swoich działań z obowiązującym prawem.

4. W przypadku korzystania z funkcji chmurowych nagrania, transkrypcje lub inne dane mogą zostać przekazane dostawcom usług wskazanym w Polityce.

5. Przed skorzystaniem z funkcji chmurowych Użytkownik powinien posiadać odpowiednią podstawę prawną oraz spełnić wymagane obowiązki informacyjne.

6. Korzystanie z trybu lokalnego nie zwalnia z obowiązku przestrzegania przepisów prawa.

§ 7. TELEMETRIA I DANE TECHNICZNE

1. Aplikacja może przysyłać do własnego backendu:

- a) losowy UUID urządzenia;
- b) model urządzenia;
- c) wersję Androida;
- d) wersję Aplikacji;
- e) nazwę użytej funkcji bez jej treści;
- f) wariant subskrypcji.

2. Telemetria nie obejmuje treści rozmów, notatek ani danych pracowników.

3. Zgodnie z audytem aktualnej wersji Aplikacja nie korzysta z Firebase, Crashlytics, AdMob ani zewnętrznego SDK reklamowego/analitycznego.

4. Dane telemetryczne mogą być przechowywane w infrastrukturze Supabase wykorzystywanej przez Operatora.

§ 8. DANE ROZLICZENIOWE

1. Zakupy są obsługiwane przez Google Play Billing.
2. Aplikacja nie przetwarza numerów kart płatniczych.
3. Backend może przetwarzać token zakupu Google Play i dane niezbędne do weryfikacji uprawnień.
4. Backend może przechowywać zużycie sekund transkrypcji, pakiety minut i liczniki zapytań AI potrzebne do egzekwowania limitów.

§ 9. UPRAWNIENIA ANDROID

Aplikacja może korzystać z: mikrofonu, usługi pierwszoplanowej typu mikrofon, wake lock, powiadomień, alarmów, uruchomienia po restarcie, Internetu, stanu sieci, biometrii i kontaktów – wyłącznie w zakresie opisanym w funkcjach Aplikacji. Kontakty mogą być użyte do opcjonalnego jednorazowego importu. Aplikacja nie korzysta z systemowego Kalendarza Google.

§ 10. KOPIE ZAPASOWE

1. Eksport/import może być szyfrowany hasłem przy użyciu AES-256/GCM i PBKDF2.
2. Aplikacja nie wysyła automatycznie pliku kopii do chmury.
3. Jeżeli Użytkownik wybierze folder synchronizowany z usługą chmurową, dalsze przetwarzanie może podlegać zasadom tej usługi.

§ 11. CELE I PODSTAWY PRAWNE

1. Cele przetwarzania mogą obejmować: świadczenie funkcji Aplikacji, transkrypcję i AI, rozliczenia i limity, bezpieczeństwo, obsługę zgłoszeń, telemetrię techniczną, obowiązki prawne oraz ustalanie, dochodzenie i obronę roszczeń.
2. Odpowiednia podstawa prawna jest ustalana dla konkretnego celu i kategorii danych. Może nią być w szczególności art. 6 ust. 1 lit. b, c, f lub a RODO, jeżeli spełnione są warunki zastosowania danej podstawy.
3. Nie należy stosować zgody jako podstawy „na wszelki wypadek”. Zgoda musi być dobrowolna, konkretna, świadoma i możliwa do wycofania, jeżeli jest stosowana.
4. W przypadku danych osób trzecich Użytkownik może mieć własne obowiązki administratora danych, w tym obowiązek ustalenia podstawy prawnej i spełnienia obowiązku informacyjnego.

§ 12. ODBIORCY I DOSTAWCY

W zależności od funkcji dane mogą być przekazywane lub udostępniane:

1. ElevenLabs – transkrypcja audio;
2. Mistral AI – podsumowania i wnioski AI;
3. Google Gemini API – podsumowania i wnioski AI;
4. Google Play / Google Play Billing – zakupy i weryfikacja zakupów;

5. Supabase – infrastruktura backendowa;
6. Google Cloud Run – hosting backendu proxy;
7. organom publicznym, jeżeli obowiązek ujawnienia wynika z prawa.

§ 13. OFICJALNE DOKUMENTY DOSTAWCÓW

Niniejsze odnośniki prowadzą do oficjalnych dokumentów dostawców. Dokumenty mogą być aktualizowane przez dostawców:

1. ElevenLabs – Privacy Policy:

<https://elevenlabs.io/privacy-policy>

2. ElevenLabs – Data Processing Addendum:

<https://elevenlabs.io/dpa>

3. Mistral AI – Data Processing Addendum:

<https://legal.mistral.ai/terms/data-processing-addendum>

4. Google APIs – Terms of Service:

<https://developers.google.com/terms/>

5. Google Cloud – Cloud Data Processing Addendum:

<https://cloud.google.com/terms/data-processing-addendum>

6. Google Play – Terms of Service:

<https://play.google.com/about/play-terms/index.html>

7. Supabase – Privacy Policy:

<https://supabase.com/privacy>

Jeżeli Użytkownik korzysta z własnego klucza API, powinien zapoznać się również z aktualnymi warunkami właściwego dostawcy.

§ 14. TRANSFERY POZA EOG

1. Korzystanie z usług zewnętrznych może wiązać się z transferem danych poza EOG.
2. Transfer może odbywać się na podstawie mechanizmu prawnego dostępnego dla konkretnego dostawcy, usługi i konfiguracji.
3. Administrator nie deklaruje konkretnego mechanizmu transferu bez jego weryfikacji dla aktualnej konfiguracji.
4. Informacje o mechanizmach transferu i zabezpieczeniach znajdują się w dokumentach dostawców wskazanych w § 13.

§ 15. BEZPIECZEŃSTWO

1. Pliki audio są szyfrowane AES-256/GCM, a klucz jest przechowywany w Android Keystore.

2. Kopie eksportowane mogą być szyfrowane AES-256/GCM z kluczem wyprowadzanym z hasła przy użyciu PBKDF2.
3. Operator stosuje środki techniczne i organizacyjne odpowiednie do ryzyka w zakresie wynikającym z faktycznej konfiguracji systemu i obowiązujących przepisów.
4. Żadne zabezpieczenie nie zapewnia absolutnej gwarancji bezpieczeństwa.
5. Użytkownik odpowiada za bezpieczeństwo urządzenia, PIN-u, haseł i własnych kluczy API.

§ 16. PRAWA OSÓB, KTÓRYCH DANE DOTYCZA

Osobie, której dane są przetwarzane, mogą przysługiwać prawa wynikające z RODO, w szczególności dostęp, sprostowanie, usunięcie, ograniczenie przetwarzania, przenoszenie danych w przypadkach przewidzianych prawem, sprzeciw wobec przetwarzania opartego na prawnie uzasadnionym interesie oraz cofnięcie zgody, jeżeli podstawą była zgoda. Przysługuje również prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

§ 17. USUWANIE DANYCH

1. Dane lokalne mogą być usuwane funkcjami Aplikacji lub przez działania systemowe.
2. Dane backendowe są usuwane zgodnie z funkcją, retencją, obowiązkami prawnymi i procedurami Operatora.
3. Dane przekazane dostawcom zewnętrznym mogą podlegać ich własnym okresom retencji i procedurom usuwania.
4. Jeżeli Aplikacja umożliwia utworzenie konta, Operator zapewnia mechanizm żądania usunięcia konta i powiązanych danych zgodny z wymaganiami Google Play oraz prawem. Adres zewnętrznego mechanizmu usunięcia konta: [DO UZUPEŁNIENIA].
5. Jeżeli Aplikacja nie umożliwia utworzenia konta, należy odpowiednio zaktualizować informacje w Google Play i niniejszej Polityce.

§ 18. BRAK REKLAM I ŚLEDZENIA REKLAMOWEGO

1. Aplikacja nie zawiera reklam.
2. Aplikacja nie wykorzystuje AAID do opisanych celów.
3. Aplikacja nie sprzedaje danych brokerom danych.
4. Aplikacja nie śledzi lokalizacji.
5. Treść rozmów i notatek nie jest wysyłana do systemu analitycznego Operatora jako telemetria.

§ 19. ZMIANY POLITYKI

1. Polityka może być aktualizowana w razie zmian prawa, funkcji, dostawców lub sposobu przetwarzania.

2. Aktualna wersja powinna być dostępna w Aplikacji i pod publicznie dostępnym adresem HTTPS.

3. Jeżeli zmiana wymaga dodatkowego poinformowania lub zgody, Administrator zastosuje sposób zgodny z prawem.

§ 20. INFORMACJA DLA UŻYTKOWNIKÓW PRZETWARZAJĄCYCH DANE PRACOWNIKÓW

Niniejsza Polityka nie zastępuje obowiązków informacyjnych Użytkownika wobec jego pracowników lub innych osób, których dane Użytkownik przetwarza. Użytkownik powinien samodzielnie zapewnić tym osobom informacje wymagane przez właściwe przepisy.

§ 21. POSTANOWIENIA KOŃCOWE

1. W przypadku rozbieżności między opisem a faktycznym działaniem aktualnej wersji Aplikacji Polityka wymaga aktualizacji.

2. Niniejsza Polityka nie stanowi gwarancji zgodności konkretnego sposobu używania Aplikacji przez Użytkownika z prawem.