POLITYKA PRYWATNOŚCI

Danger Studio App i serwisu Danger Studio

Data ostatniej aktualizacji: 30 października 2026 r.

Administrator danych osobowych: DANGER STUDIO, Polska
e-mail: dangerstudio.app@gmail.com • www.dangerstudioapp.com

Spis treści

1. Postanowienia ogólne....3
2. Zakres usług....3
3. Konto użytkownika....4
4. Wix....4
5. Render – infrastruktura backendu aplikacji....5
6. Logowanie do Danger Studio App....6
7. Subskrypcje i dostęp do aplikacji....6
8. Płatności....6
9. Dane przechowywane w Supabase....7
10. Dane przechowywane lokalnie na komputerze użytkownika....8
11. Czat wykorzystujący sztuczną inteligencję....9
12. Analiza dźwięku i dostęp do mikrofonuAnaliza dźwięku i dostęp do mikrofonu....10
13. Aktualizacje Aplikacji....11
14. Cele przetwarzania danych....11
15. Podstawy prawne przetwarzania....12
16. Pliki cookies i technologie podobne....13
17. Reklamy, marketing i profilowanie....14
18. Odbiorcy danych....14
19. Przekazywanie danych poza Europejski Obszar Gospodarczy....15
20. Okres przechowywania danych....15
21. Usunięcie konta....17
22. Prawa użytkownika....18
23. Prawo do wniesienia skargi....18
24. Wiek użytkowników....19
25. Bezpieczeństwo danych....19
26. Brak sprzedaży danych....19
27. Zautomatyzowane podejmowanie decyzji....19
28. Dostępność terytorialna....20
29. Zmiany Polityki Prywatności....20
30. Zewnętrzni dostawcy usług....20
31. Kontakt....23
32. Podsumowanie sposobu przetwarzania danych....23

1. Postanowienia ogólne

Niniejsza Polityka Prywatności określa zasady przetwarzania danych osobowych użytkowników strony internetowej www.dangerstudioapp.com oraz aplikacji komputerowej Danger Studio App, przeznaczonej dla komputerów z systemem Windows.

Administratorem danych osobowych jest:

DANGER STUDIO DAWID ANGERHOEFER, Polska

Wlewsk 23, 13-230 Lidzbark

REGON: 386964434

NIP: 5711721191

e-mail: **dangerstudio.app@gmail.com**

strona internetowa: **https://www.dangerstudioapp.com/**

W dalszej części dokumentu DANGER STUDIO może być określane jako „Administrator", „DANGER STUDIO" lub „my".

W sprawach dotyczących ochrony danych osobowych i prywatności użytkownik może skontaktować się z Administratorem za pomocą adresu dangerstudio.app@gmail.com.

DANGER STUDIO dokłada starań, aby ograniczać zakres przetwarzanych danych do informacji niezbędnych do świadczenia usług, obsługi kont użytkowników, realizacji płatności, zapewnienia działania Aplikacji oraz udostępniania jej funkcji.

Znaczna część danych związanych z działaniem Danger Studio App jest przechowywana lokalnie na komputerze użytkownika.

2. Zakres usług

DANGER STUDIO świadczy usługę polegającą na umożliwieniu użytkownikom korzystania z Aplikacji komputerowej Danger Studio App oraz powiązanych z nią funkcji internetowych.

Danger Studio App może być dostępna zarówno w ramach **planu bezpłatnego**, jak i **planów płatnych**.

Zakres dostępnych funkcji może różnić się w zależności od wybranego planu.

Korzystanie z planu bezpłatnego nie wymaga posiadania aktywnej płatnej subskrypcji, natomiast dostęp do funkcji objętych planami płatnymi wymaga aktywnej subskrypcji.

Proces korzystania z usługi może obejmować w szczególności:

- utworzenie konta na stronie internetowej DANGER STUDIO,
- korzystanie z funkcji dostępnych w planie bezpłatnym,
- zakup wybranego planu płatnego,
- uzyskanie dostępu do dodatkowych funkcji objętych subskrypcją,
- pobranie i uruchomienie Danger Studio App,
- logowanie do Aplikacji,
- weryfikację konta oraz, w przypadku funkcji płatnych, statusu subskrypcji,
- korzystanie z funkcji Aplikacji odpowiednich dla danego planu.

3. Konto użytkownika

Korzystanie z Danger Studio App wymaga utworzenia konta za pośrednictwem strony internetowej https://www.dangerstudioapp.com/.

Strona internetowa DANGER STUDIO została utworzona i jest obsługiwana z wykorzystaniem infrastruktury platformy Wix.

Podczas tworzenia oraz korzystania z konta mogą być przetwarzane w szczególności następujące dane:

- Imię.
- Nazwisko.
- Oświadczenie o ukończeniu 18 lat.
- Adres e-mail.
- Nick lub nazwa użytkownika.
- Dane związane z kontem użytkownika.
- Dane dotyczące wybranego planu oraz, jeżeli ma to zastosowanie, posiadanej subskrypcji.
- Informacje niezbędne do logowania i uwierzytelnienia użytkownika.

Konto możesz utworzyć i logować się przez Wix przy użyciu adresu e-mail i hasła albo wybrać Google lub Facebook. Wybrany dostawca uwierzytelnia Cię i przekazuje do Wix dane profilu w zakresie wyświetlanym podczas łączenia konta. Logowanie społecznościowe jest opcjonalne. Usunięcie konta Danger Studio nie usuwa konta Google ani Facebook. Zasady dostawców opisują polityki prywatności Google: https://policies.google.com/privacy?hl=pl oraz Facebook: https://www.facebook.com/privacy/policy/.

DANGER STUDIO posiada dostęp do danych użytkowników w zakresie niezbędnym do obsługi konta i świadczonych usług.

Dane konta są obsługiwane z wykorzystaniem infrastruktury Wix. Do obsługi konta Aplikacji synchronizujemy z Wix do Supabase identyfikator członka Wix, adres e-mail, nazwę profilu i adres zdjęcia profilowego, o ile są dostępne. Hasła Wix ani hasła dostawców logowania społecznościowego nie są kopiowane do Supabase.

Usługa jest przeznaczona dla osób, które ukończyły 18 lat. Przy rejestracji wymagamy oświadczenia o pełnoletności i zapoznaniu się z Regulaminem. Przy rejestracji przez Google lub Facebook oświadczenie następuje w dodatkowym kroku po uwierzytelnieniu u dostawcy, przed zalogowaniem do witryny.

Domyślnie profil społecznościowy jest widoczny dla innych zalogowanych członków witryny. Widoczne mogą być nazwa wyświetlana, awatar, data dołączenia, liczniki obserwowania i dodane informacje o sobie. Osoby niezalogowane nie mogą oglądać profili. Widoczność można zmienić w ustawieniach na prywatną; profil przestaje wtedy być dostępny innym członkom przez link do profilu. Nie usuwa to konta ani danych potrzebnych do jego obsługi.

4. Wix

DANGER STUDIO korzysta z platformy Wix.com w szczególności w celu:

- Prowadzenia strony internetowej.
- Obsługi rejestracji użytkowników.
- Obsługi logowania.
- Zarządzania kontami użytkowników.
- Udostępniania użytkownikom dostępu do treści i usług.

- Obsługi procesu zakupu subskrypcji.
- Umożliwienia weryfikacji uprawnień użytkownika do korzystania z Danger Studio App.

Za pośrednictwem infrastruktury Wix mogą być przetwarzane w szczególności:

- Imię.
- Nazwisko.
- Adres e-mail.
- Oświadczenie o ukończeniu 18 lat.
- Dane konta.
- Dane dotyczące logowania.
- Informacje związane z subskrypcją.
- Adres zamieszkania, adres rozliczeniowy lub inne dane do faktury, jeżeli użytkownik poda je podczas zakupu lub rozliczenia.
- Dane techniczne dotyczące korzystania ze strony internetowej.
- Adres IP.
- Informacje dotyczące urządzenia, przeglądarki i sesji.
- Dane niezbędne do zapewnienia bezpieczeństwa strony i procesu logowania.

Dane te mogą być przechowywane przy wykorzystaniu infrastruktury informatycznej udostępnianej przez Wix i jego podwykonawców.

DANGER STUDIO może uzyskiwać dostęp do danych użytkowników za pomocą panelu administracyjnego Wix w zakresie niezbędnym do świadczenia usług, obsługi użytkowników, zarządzania kontami, realizacji umowy, obsługi subskrypcji oraz wystawiania dokumentów sprzedażowych.

Wix może również przetwarzać określone dane zgodnie z własną polityką prywatności oraz warunkami świadczenia usług.

5. Render – infrastruktura backendu aplikacji

DANGER STUDIO korzysta z usług Render w celu zapewnienia infrastruktury backendowej niezbędnej do działania Danger Studio App.

Backend działający w infrastrukturze Render pośredniczy w komunikacji pomiędzy Aplikacją użytkownika a innymi systemami i usługami wykorzystywanymi przez DANGER STUDIO.

Render może uczestniczyć technicznie w obsłudze w szczególności:

- Logowania użytkownika.
- Weryfikacji konta i subskrypcji.
- Obsługi sesji.
- Obsługi rankingu.
- Pobierania danych niezbędnych do działania Aplikacji.
- Komunikacji z innymi usługami wykorzystywanymi przez Danger Studio App.
- Obsługi funkcji czatu AI.

W przypadku korzystania z czatu AI wiadomość użytkownika jest przekazywana w następującym przepływie:

Danger Studio App → backend Render → OpenAI API.

Render pełni w tym procesie rolę infrastruktury technicznej pośredniczącej w przekazaniu danych niezbędnych do realizacji danej funkcji.

Render może przetwarzać dane zgodnie z zasadami ochrony danych i warunkami świadczenia swoich usług.

6. Logowanie do Danger Studio App

Każde uruchomienie Danger Studio App wymaga uwierzytelnienia użytkownika. Proces logowania jest powiązany ze stroną internetową DANGER STUDIO.

Logowanie służy między innymi:

- Potwierdzeniu tożsamości użytkownika.
- Sprawdzeniu istnienia aktywnego konta.
- Sprawdzeniu rodzaju planu oraz, jeżeli ma to zastosowanie, statusu subskrypcji.
- Potwierdzeniu prawa do korzystania z Aplikacji.
- Zabezpieczeniu Aplikacji przed dostępem osób nieuprawnionych.

Aplikacja może komunikować się z systemami internetowymi DANGER STUDIO w zakresie niezbędnym do dokonania powyższej weryfikacji.

7. Subskrypcje i dostęp do aplikacji

Danger Studio App może być oferowana w ramach planu bezpłatnego oraz planów płatnych.

Plan bezpłatny umożliwia korzystanie z wybranych funkcji Aplikacji bez konieczności posiadania aktywnej płatnej subskrypcji.

Dostęp do dodatkowych lub rozszerzonych funkcji może wymagać wykupienia płatnej subskrypcji.

Użytkownik może wykupić w szczególności:

- subskrypcję miesięczną,
- subskrypcję roczną.

Zakres funkcji dostępnych w poszczególnych planach jest określany w aktualnej ofercie DANGER STUDIO.

Status subskrypcji może być sprawdzany przy logowaniu lub korzystaniu z funkcji wymagających aktywnego planu płatnego.

DANGER STUDIO może przetwarzać informacje niezbędne do ustalenia zakresu dostępu użytkownika do usługi, w szczególności:

- rodzaj planu,
- status subskrypcji,
- datę rozpoczęcia subskrypcji,
- datę jej wygaśnięcia lub odnowienia,
- status płatności,
- identyfikator transakcji lub subskrypcji.

8. Płatności

Płatności obsługuje Stripe lub PayPal, zależnie od wybranej metody. Apple Pay i Google Pay są w naszej konfiguracji obsługiwane przez Stripe. Metody dostępne dla konkretnego planu są wskazane podczas zakupu. Dane

niezbędne do realizacji i rozliczenia transakcji przetwarzają Wix i właściwy operator. W związku z płatnością operator może przetwarzać między innymi:

- Imię i nazwisko.
- Adres e-mail.
- Dane rozliczeniowe.
- Informacje dotyczące sposobu płatności.
- Dane karty płatniczej.
- Kwotę i walutę transakcji.
- Datę transakcji.
- Informacje dotyczące subskrypcji.
- Adres IP.
- Dane służące zapobieganiu oszustwom i nadużyciom.

DANGER STUDIO nie przechowuje pełnych danych kart płatniczych użytkowników. Pełne dane dotyczące instrumentów płatniczych obsługują właściwi dostawcy płatności.

DANGER STUDIO może mieć dostęp do ograniczonych informacji dotyczących transakcji, niezbędnych do:

- Potwierdzenia płatności.
- Ustalenia statusu subskrypcji.
- Obsługi użytkownika.
- Rozpatrywania reklamacji.
- Realizacji obowiązków księgowych i prawnych.

Operatorzy mogą działać jako odrębni administratorzy dla własnych celów płatniczych, bezpieczeństwa i obowiązków prawnych. Zasady ich przetwarzania, retencji i transferów opisują polityki prywatności Stripe: https://stripe.com/privacy oraz PayPal: https://www.paypal.com/pl/legalhub/paypal/privacy-full.

9. Dane przechowywane w Supabase

DANGER STUDIO korzysta z infrastruktury Supabase w celu przechowywania i obsługi danych niezbędnych do działania wybranych funkcji Danger Studio App.

W Supabase mogą być przechowywane w szczególności:

- Adres e-mail.
- Identyfikatory użytkownika i konta.
- Nick lub nazwa użytkownika.
- Informacje dotyczące awatara.
- Informacje dotyczące planu oraz, jeżeli ma to zastosowanie, subskrypcji.
- Dane techniczne dotyczące sesji i urządzeń.
- Informacje dotyczące postępów użytkownika.
- Dane wykorzystywane w rankingu.
- Informacje niezbędne do obsługi dziennego limitu korzystania z czatu AI.

Opcjonalne statystyki korzystania z lekcji, programów, ćwiczeń, gier i narzędzi są domyślnie wyłączone. Możesz włączyć ich zapisywanie na stronie „Twoje statystyki”, wyrażając zgodę, oraz w tym samym miejscu ją wycofać.

Brak zgody nie wyłącza podstawowych funkcji Aplikacji. Obsługa konta, bezpieczeństwa, postępu lekcji, odblokowanych poziomów i rankingu jest odrębna od opcjonalnego zapisywania statystyk aktywności.

Statystyki te mogą obejmować w szczególności:

- identyfikator konta użytkownika,
- nazwę zdarzenia lub wykonanej aktywności,
- identyfikator Aplikacji, lekcji, programu, gry lub strony,
- datę i czas zdarzenia,
- czas korzystania z danej funkcji,
- wersję Aplikacji,
- wyniki liczbowe wykonywanych ćwiczeń, takie jak tempo, liczba trafień lub celność,
- wyniki uzyskiwane w grach,
- techniczne informacje dotyczące sesji.

Dane dotyczące aktywności i wyników mogą być przypisane do konta użytkownika. Są one wykorzystywane w celu prezentowania użytkownikowi jego własnych postępów i historii aktywności oraz w celu tworzenia zbiorczych statystyk umożliwiających DANGER STUDIO ocenę sposobu korzystania z poszczególnych lekcji, programów i gier oraz rozwój i poprawę działania usługi.

Panel użytkownika prezentuje podsumowania jego aktywności i wyników. Widok całej historii łączy bieżące dane szczegółowe ze starszymi osobistymi podsumowaniami kategorii. DANGER STUDIO korzysta również ze zbiorczych zestawień dotyczących popularności funkcji i wyników ćwiczeń w celu rozwijania usługi. Zasady przechowywania opisano w rozdziale 20.

W ramach statystyk nie są przesyłane ani przechowywane nagrania audio lub próbki dźwięku z mikrofonu, treść własnych plików TAB użytkownika ani ścieżki prowadzące do takich plików na komputerze użytkownika.

Dane techniczne dotyczące sesji i urządzeń są wykorzystywane w szczególności w celu zapewnienia bezpieczeństwa konta, uwierzytelnienia użytkownika oraz zarządzania aktywnymi sesjami.

Treść rozmów prowadzonych za pomocą czatu AI nie jest przechowywana w Supabase.

Dane przechowywane w Supabase służą obsłudze konta, zarządzaniu dostępem, planem lub subskrypcją, bezpieczeństwu konta, zapisywaniu postępu lekcji i wyników oraz prowadzeniu rankingu. Po wyrażeniu odrębnej zgody przetwarzamy także opcjonalne statystyki aktywności w celu prezentowania użytkownikowi jego historii i tworzenia zbiorczych analiz korzystania z funkcji Aplikacji.

DANGER STUDIO nie sprzedaje tych danych podmiotom trzecim oraz nie wykorzystuje ich do personalizacji reklam.

10. Dane przechowywane lokalnie na komputerze użytkownika

W celu logowania, ochrony konta i zarządzania aktywnymi urządzeniami przetwarzane są dane sesji, informacje o aktywnym urządzeniu oraz daty aktywności i wygaśnięcia sesji. Lokalnie dane logowania są zabezpieczane w ramach mechanizmów systemu Windows.

Część danych Danger Studio App jest przechowywana wyłącznie lokalnie na komputerze użytkownika. Mogą to być w szczególności:

- Historia rozmów prowadzonych za pomocą funkcji AI.
- Ustawienia aplikacji.
- Dane techniczne niezbędne do działania programu.
- Inne lokalne informacje związane z korzystaniem z Aplikacji.

W przypadku chwilowego braku połączenia z usługami internetowymi Aplikacja może lokalnie przechowywać ograniczoną kolejkę niewysłanych zdarzeń dotyczących statystyk korzystania z Aplikacji. Kolejka służy wyłącznie do ponowienia wysyłki odpowiednich informacji po odzyskaniu połączenia.

Kolejka ma ograniczony zakres i jest powiązana z bieżącą sesją użytkownika. Jest czyszczona przy wylogowaniu, tak aby niewysłane zdarzenia dotyczące jednego konta nie zostały później przypisane do aktywności innego użytkownika korzystającego z tego samego komputera.

Wyłączenie przełącznika zapisywania nowych statystyk wstrzymuje nowe zapisy. Dotychczasowa historia pozostaje dostępna, a zgoda na jej przechowywanie i podsumowywanie pozostaje aktywna. Starsze dane mogą nadal zostać zastąpione podsumowaniami zgodnie z zasadami retencji. Wstrzymanie nowych zapisów nie jest wycofaniem zgody.

Aby wycofać zgodę, wybierz „Wycofaj zgodę i usuń statystyki" na stronie „Twoje statystyki" i potwierdź operację. Wycofanie zatrzymuje zapisy i usuwa szczegółowe zdarzenia oraz starsze osobiste podsumowania. Usuwane dane nie są najpierw przenoszone do globalnych sum. Operacja nie pomniejsza już zgromadzonych niezależnych globalnych podsumowań i nie usuwa postępu lekcji, odblokowanych poziomów ani wyników rankingu.

Wstrzymanie i wycofanie natychmiast zatrzymują lokalne zbieranie nowych zdarzeń i usuwają niewysłaną kolejkę. Gdy urządzenie jest offline, przekazanie decyzji do serwera jest ponawiane po odzyskaniu połączenia. Usunięcie danych na serwerze wymaga skutecznego przekazania decyzji. Ponowne włączenie statystyk wymaga Twojego działania.

DANGER STUDIO nie posiada bezpośredniego dostępu do plików znajdujących się lokalnie na komputerze użytkownika. Użytkownik może samodzielnie zarządzać określonymi lokalnymi danymi.

Historia rozmów AI może zostać usunięta:

- Z poziomu Danger Studio App.
- Ręcznie poprzez usunięcie odpowiednich plików na komputerze użytkownika.

Usunięcie danych lokalnych może być niezależne od usunięcia konta internetowego.

11. Czat wykorzystujący sztuczną inteligencję

Wiadomość wysłana w czacie AI jest przekazywana w następującym przepływie: Aplikacja Danger Studio App → backend Render → OpenAI API. Treść wiadomości przekazujemy do wygenerowania odpowiedzi. Dostawca przetwarza ją również w zakresie opisanych niżej zasad bezpieczeństwa usługi i przeciwdziałania nadużyciom.

Do OpenAI wysyłamy bieżące pytanie i instrukcję systemową. Nie dołączamy osobnych pól identyfikujących konto, takich jak adres e-mail, identyfikator konta lub urządzenia ani adres IP użytkownika. Sam użytkownik może jednak wpisać dane w treści pytania. Dostawca otrzymuje żądanie z naszego backendu Render i dane techniczne tego połączenia. Nie przekazujemy poprzednich wiadomości z lokalnej historii, materiałów lekcji ani statystyk użytkownika.

DANGER STUDIO nie wykorzystuje treści rozmów do:

- Profilowania reklamowego.
- Prowadzenia reklam.
- Sprzedaży danych użytkowników.
- Prowadzenia kampanii marketingowych.

Historia rozmów widoczna w Danger Studio App jest zapisywana lokalnie na komputerze użytkownika. Należy jednak pamiętać, że treść konkretnego zapytania oraz odpowiedzi jest przetwarzana przez OpenAI w celu wykonania usługi.

Wyłączyliśmy zapisywanie odpowiedzi jako przechowywanego zasobu API. Nie oznacza to wyłączenia logów bezpieczeństwa dostawcy. Zgodnie z zasadami OpenAI API dane wejściowe i wyjściowe nie są domyślnie wykorzystywane do trenowania modeli, chyba że klient API dobrowolnie je udostępni. OpenAI może przechowywać treści w logach bezpieczeństwa i przeciwdziałania nadużyciom domyślnie do 30 dni, a dłużej, jeśli wymagają tego przepisy prawa lub ochrona usług i osób trzecich, zgodnie z zasadami stosowanej usługi API: https://developers.openai.com/api/docs/guides/your-data.

Użytkownik powinien unikać przekazywania za pomocą czatu AI:

- Haseł.
- Danych kart płatniczych.
- Numerów dokumentów tożsamości.
- Szczególnie wrażliwych danych osobowych.
- Poufnych informacji, których przekazanie nie jest konieczne do korzystania z funkcji.
- Danych innych osób.

OpenAI przetwarza dane zgodnie z własnymi zasadami prywatności i zasadami dotyczącymi usług API.

12. Analiza dźwięku i dostęp do mikrofonu

Danger Studio App zawiera autorski system służący do bieżącej analizy poprawności wykonywania ćwiczeń muzycznych.

W celu korzystania z tej funkcji Aplikacja może uzyskiwać dostęp do mikrofonu lub innego urządzenia wejściowego audio podłączonego do komputera użytkownika.

Dźwięk jest przetwarzany lokalnie i wyłącznie w czasie rzeczywistym, w zakresie niezbędnym do oceny poprawności wykonywanego ćwiczenia.

Analizowany dźwięk:

- Nie jest nagrywany ani archiwizowany przez DANGER STUDIO.
- Nie jest przesyłany na serwery DANGER STUDIO.
- Nie jest przesyłany do OpenAI.
- Nie jest przesyłany do Supabase.
- Nie jest wykorzystywany do identyfikacji użytkownika.
- Nie jest wykorzystywany do celów reklamowych lub marketingowych.
- Nie jest przechowywany po zakończeniu bieżącej analizy.

Jeżeli przetwarzany sygnał audio w określonych okolicznościach mógłby stanowić dane osobowe, jego przetwarzanie odbywa się wyłącznie w zakresie niezbędnym do udostępnienia użytkownikowi funkcji analizy wykonywanego ćwiczenia, na podstawie art. 6 ust. 1 lit. b RODO, tj. w celu wykonania usługi świadczonej użytkownikowi.

Dostęp systemu Windows do mikrofonu może dodatkowo wymagać zgody lub zezwolenia użytkownika na poziomie systemu operacyjnego. Użytkownik może zarządzać takim dostępem w ustawieniach prywatności systemu Windows.

DANGER STUDIO nie tworzy bazy nagrań głosowych ani nagrań gry użytkowników.

Brak zapisywania i przesyłania sygnału audio nie oznacza, że wyniki wykonywanego ćwiczenia nie mogą zostać zapisane na koncie użytkownika. Po zakończeniu analizy Aplikacja może zapisać wynikające z niej dane liczbowe dotyczące przebiegu i wyniku ćwiczenia.

Może to obejmować w szczególności wyniki ćwiczeń wykonywanych przy użyciu funkcji Danger Checker oraz Danger Tabs, takie jak tempo, liczba poprawnych lub błędnych trafień, celność albo inne wartości opisujące rezultat ćwiczenia.

Do systemów DANGER STUDIO mogą być zatem przekazywane wyniki liczbowe ćwiczenia, natomiast sam sygnał audio, nagranie ani próbki dźwięku z mikrofonu nie są w tym celu przesyłane ani archiwizowane.

13. Aktualizacje Aplikacji

Danger Studio App może okresowo sprawdzać dostępność nowych wersji Aplikacji oraz umożliwiać pobieranie aktualizacji.

W związku z obsługą procesu aktualizacji mogą być przetwarzane w szczególności:

- aktualna wersja Aplikacji,
- techniczny identyfikator urządzenia,
- informacja o aktywnej sesji użytkownika,
- dane techniczne niezbędne do sprawdzenia i pobrania aktualizacji.

Dane te są wykorzystywane wyłącznie w zakresie niezbędnym do sprawdzenia dostępności aktualizacji, weryfikacji uprawnień użytkownika oraz bezpiecznego udostępnienia odpowiedniej wersji instalatora.

14. Cele przetwarzania danych

Dane osobowe użytkowników mogą być przetwarzane w szczególności w celu:

- Utworzenia konta.
- Obsługi konta użytkownika.
- Uwierzytelnienia użytkownika.
- Umożliwienia logowania.
- Świadczenia usług DANGER STUDIO.
- Wykonywania umowy zawartej z użytkownikiem.
- Realizacji i obsługi subskrypcji.
- Realizacji płatności.
- Weryfikacji prawa dostępu do Aplikacji.
- Zapisywania postępów użytkownika.
- Prezentowania postępu lekcji i wyników niezbędnych do działania wybranych funkcji oraz, po wyrażeniu odrębnej zgody, opcjonalnej historii statystyk aktywności.
- Po wyrażeniu zgody na opcjonalne statystyki: tworzenia zbiorczych analiz dotyczących korzystania z lekcji, programów, ćwiczeń i gier w celu oceny działania oraz rozwoju Danger Studio App.
- Prowadzenia rankingu.
- Zapewnienia funkcji czatu AI.
- Zapewnienia działania strony internetowej.

- Zapewnienia działania Aplikacji.
- Obsługi, sprawdzania dostępności i bezpiecznego udostępniania aktualizacji Danger Studio App.
- Zapewnienia bezpieczeństwa systemów.
- Zapobiegania nadużyciom.
- Świadczenia pomocy technicznej.
- Rozpatrywania reklamacji.
- Realizacji obowiązków podatkowych, księgowych i prawnych.
- Ustalenia, dochodzenia lub obrony roszczeń.

15. Podstawy prawne przetwarzania

Podanie danych niezbędnych do utworzenia konta, logowania i obsługi subskrypcji jest wymogiem umownym. Ich niepodanie uniemożliwia korzystanie z funkcji wymagających konta i dostępu online.

DANGER STUDIO przetwarza dane osobowe wyłącznie wtedy, gdy istnieje odpowiednia podstawa prawna.

15.1. Wykonanie umowy – art. 6 ust. 1 lit. b RODO

Na tej podstawie przetwarzane są dane niezbędne do:

- Utworzenia i obsługi konta.
- Uwierzytelnienia użytkownika.
- Umożliwienia logowania.
- Sprawdzenia rodzaju planu oraz, jeżeli ma to zastosowanie, statusu subskrypcji.
- Zapewnienia dostępu do Danger Studio App.
- Zapewnienia sprawdzania i udostępniania aktualizacji Aplikacji.
- Zapisywania postępu lekcji i odblokowanych poziomów potrzebnych do działania tych funkcji.
- Zapisywania i prezentowania wyników niezbędnych do działania wybranej funkcji Aplikacji. Nie obejmuje to opcjonalnej historii statystyk aktywności.
- Udostępnienia funkcji związanych z rankingiem.
- Realizacji funkcji czatu AI.
- Realizacji bieżącej, lokalnej analizy dźwięku niezbędnej do działania funkcji ćwiczeń.

15.2. Obowiązek prawny – art. 6 ust. 1 lit. c RODO

Na tej podstawie mogą być przetwarzane dane, których zachowanie jest wymagane przez przepisy prawa, w szczególności przepisy:

- Podatkowe.
- Księgowe.
- Dotyczące rozliczeń i dokumentowania transakcji.

15.3. Prawnie uzasadniony interes – art. 6 ust. 1 lit. f RODO

Na tej podstawie dane mogą być przetwarzane w szczególności w celu:

- Zapewnienia bezpieczeństwa usług.
- Ochrony przed nadużyciami.
- Zabezpieczania systemów informatycznych.

- Przeciwdziałania oszustwom.
- Obsługi roszczeń.
- Obrony przed roszczeniami.
- Zapewnienia prawidłowego działania infrastruktury technicznej.

Prawnie uzasadnione interesy DANGER STUDIO w tym zakresie obejmują ochronę użytkowników i systemów przed nadużyciami, utrzymanie bezpieczeństwa i działania infrastruktury oraz ustalenie, dochodzenie lub obronę roszczeń. Opcjonalne statystyki aktywności opisane w rozdziale 9 są przetwarzane na podstawie odrębnej zgody, zgodnie z rozdziałem 15.4.

15.4. Zgoda – art. 6 ust. 1 lit. a RODO

Na podstawie dobrowolnej zgody przetwarzamy opcjonalne statystyki aktywności: szczegółowe zdarzenia, osobiste podsumowania kategorii oraz dane wykorzystywane do tworzenia zbiorczych analiz rozwoju usługi. Statystyki są domyślnie wyłączone; odmowa nie wyłącza podstawowych funkcji Aplikacji. Zgoda na statystyki Aplikacji jest odrębna od wyborów dotyczących cookies strony.

Zgodę możesz wycofać w dowolnym momencie przez „Wycofaj zgodę i usuń statystyki” na stronie „Twoje statystyki”. Wycofanie nie wpływa na zgodność z prawem przetwarzania dokonanego przed jego wycofaniem. Sama pauza nowych zapisów nie wycofuje zgody na przechowywanie i podsumowywanie dotychczasowej historii. Szczegóły skutków decyzji opisano w rozdziałach 10 i 20.

16. Pliki cookies i technologie podobne

Strona internetowa DANGER STUDIO funkcjonuje przy wykorzystaniu infrastruktury Wix i korzysta z plików cookies oraz podobnych technologii. Są one wykorzystywane między innymi w celu:

- Zapewnienia prawidłowego działania strony.
- Utrzymania sesji użytkownika.
- Umożliwienia logowania.
- Zapewnienia bezpieczeństwa.
- Zapamiętywania określonych ustawień.
- Obsługi kont użytkowników.
- Technicznej obsługi procesu płatności.

Niektóre pliki cookies mogą być niezbędne do prawidłowego działania strony i nie wymagają dodatkowej zgody, jeżeli są wykorzystywane wyłącznie w celu świadczenia usługi żądanej przez użytkownika.

Preferencjami cookies zarządzasz w polskim panelu CookieYes na stronie. Dostępne są opcje „Dostosuj”, „Odrzuć wszystkie”, „Akceptuj wszystko” i „Zapisz moje preferencje”. Panel można ponownie otworzyć przez ikonę ustawień cookies. Niezbędne mechanizmy pozostają aktywne. W panelu znajdziesz informacje o wykrytych plikach i dostępnych wyborach. Możesz również zarządzać plikami cookies w ustawieniach przeglądarki.

CookieYes rejestruje wybory odwiedzających, w tym status akceptacji lub odrzucenia, wybrane kategorie, identyfikator oraz datę i czas UTC i dowód wyboru. Stosowane maskowanie adresu IP nie oznacza gwarantowanej anonimowości. Zasady przechowywania rejestru opisano w rozdziale 20.

Witryna wykorzystuje mechanizmy Wix i Cloudflare związane z sesją i bezpieczeństwem, a formularz rejestracyjny jest chroniony przed botami przez Google reCAPTCHA. Ustawienia cookies strony są odrębne od zgody na opcjonalne statystyki ćwiczeń w Aplikacji.

Plik Wix „fedops.logger.defaultOverrides” przechowuje krótkotrwałe ustawienia diagnostyki działania komponentów Wix. Jego przypisanie do kategorii jest wyjaśniane z dostawcą; w panelu jest obecnie wskazany jako „Bez kategorii”.

Strona usuwania konta korzysta z pamięci sesyjnej przeglądarki do zachowania potwierdzenia żądania, etapu operacji, czasu ponownego wysłania kodu i pseudonimowego oznaczenia konta. Nie zapisuje tam hasła ani kodu z e-maila i nie używa tych informacji do analityki lub reklamy.

17. Reklamy, marketing i profilowanie

Danger Studio App oraz usługi DANGER STUDIO:

- Nie wyświetlają użytkownikom reklam w Aplikacji.
- Nie personalizują reklam.
- Nie sprzedają danych użytkowników reklamodawcom.
- Nie prowadzą newslettera.
- Nie wysyłają marketingowych powiadomień push.
- Nie wykorzystują danych użytkowników do mierzenia skuteczności kampanii reklamowych.
- Nie prowadzą profilowania użytkowników na potrzeby reklamy behawioralnej.

Dane dotyczące postępów w nauce, rankingu i korzystania z aplikacji nie są wykorzystywane przez DANGER STUDIO do tworzenia profili reklamowych.

18. Odbiorcy danych

W zakresie koniecznym do działania usługi dane mogą być przetwarzane przez zewnętrznych dostawców technologii. Do głównych dostawców należą:

Dostawca	Zakres / rola
Wix	Hosting strony internetowej, konta użytkowników, rejestracja, logowanie oraz infrastruktura strony.
Render	Infrastruktura backendu Danger Studio App oraz techniczne pośredniczenie w komunikacji pomiędzy Aplikacją a innymi usługami.
Stripe i PayPal	Obsługa płatności i subskrypcji zależnie od wybranej metody. Apple Pay i Google Pay są w naszej konfiguracji obsługiwane przez Stripe.
Supabase	Przechowywanie i obsługa danych konta, subskrypcji, sesji, postępu lekcji, rankingu oraz, po wyrażeniu zgody, opcjonalnych statystyk aktywności i osobistych podsumowań kategorii.
Cloudflare R2	Przechowywanie i dostarczanie instalatorów oraz filmów lekcji. Obsługa pobierania obejmuje dane techniczne żądań.
OpenAI	Przetwarzanie wiadomości w ramach funkcji czatu AI.
Google	Opcjonalne logowanie przez Google oraz ochrona formularza rejestracyjnego przez reCAPTCHA. Zakres i rola dostawcy zależą od danej usługi.
Meta / Facebook	W przypadku korzystania z logowania za pomocą konta Facebook.

Dostawca	Zakres / rola
CookieYes Limited	Zarządzanie preferencjami cookies i rejestrowanie wyborów odwiedzających w imieniu DANGER STUDIO.

Dane mogą być również udostępniane podmiotom, jeżeli obowiązek taki wynika z przepisów prawa lub wiążącego żądania właściwego organu.

19. Przekazywanie danych poza Europejski Obszar Gospodarczy

Podstawowy backend Render działa we Frankfurcie w Niemczech, a projekt bazy Supabase w Irlandii (eu-west-1). W konfiguracji obu używanych zasobów Cloudflare R2 do filmów i instalatorów wskazano preferowaną lokalizację Eastern Europe (EEUR). To ustawienie nie gwarantuje przechowywania wszystkich danych w tym obszarze ani ograniczenia ich przetwarzania do UE. Europejska lokalizacja tych usług nie wyklucza operacji poza Europejskim Obszarem Gospodarczym, np. wsparcia technicznego, obsługi kont dostawców lub usług ich dalszych podwykonawców. Nie deklarujemy ograniczenia wszystkich operacji Wix, Cloudflare, OpenAI ani pozostałych dostawców do UE.

Dane przetwarzane na nasze zlecenie podlegają właściwym umowom powierzenia. W odniesieniu do transferów poza EOG umowy Render, Supabase, Cloudflare, OpenAI i CookieYes przewidują odpowiednie zabezpieczenia, w tym standardowe klauzule umowne Komisji Europejskiej tam, gdzie mają zastosowanie, lub właściwe decyzje o odpowiednim stopniu ochrony. Dokumenty dostawców: Render https://render.com/dpa; Supabase https://supabase.com/legal/customer-resources/data-processing-addendum; Cloudflare https://www.cloudflare.com/cloudflare-customer-dpa/; OpenAI https://openai.com/policies/data-processing-addendum/; CookieYes https://www.cookieyes.com/dpa/.

Umowa powierzenia Wix opisuje transfer do Izraela na podstawie decyzji o odpowiednim stopniu ochrony oraz zabezpieczenia dalszych transferów, w tym standardowe klauzule umowne: https://www.wix.com/about/privacy-dpa-users. Dokumenty Stripe opisują zabezpieczenia transferów, w tym standardowe klauzule umowne: https://stripe.com/legal/dpa oraz https://stripe.com/legal/dta. PayPal opisuje między innymi wiążące reguły korporacyjne dla transferów wewnątrz grupy: https://www.paypal.com/pl/legalhub/paypal/bcr.

CookieYes Limited ma siedzibę w Wielkiej Brytanii i korzysta z podwykonawców w różnych państwach. Nie gwarantujemy wyłącznego przetwarzania danych tego narzędzia w EOG. Informacje o stosowanych zabezpieczeniach transferów i możliwości uzyskania ich kopii są dostępne pod adresem dangerstudio.app@gmail.com.

20. Okres przechowywania danych

DANGER STUDIO stosuje zasadę ograniczenia przechowywania danych i nie przechowuje danych osobowych dłużej, niż jest to konieczne do realizacji celu, w którym zostały zebrane.

Poszczególne kategorie danych są przechowywane według następujących zasad:

Logi bezpieczeństwa

Ograniczona historia zdarzeń bezpieczeństwa konta obejmuje rodzaj zdarzenia, krótki opis, informacje o Aplikacji i datę zdarzenia. Wpisy tej historii nie obejmują treści czatu, nagrań dźwiękowych, adresu IP, geolokalizacji ani modelu urządzenia. Wpisy starsze niż 30 dni są automatycznie usuwane podczas codziennego zadania porządkowania. Usunięcie następuje w najbliższym cyklu po przekroczeniu tego okresu, a nie dokładnie w chwili upływu 30 dni. Zasada dotyczy tej historii konta i nie określa retencji wszystkich logów infrastruktury dostawców.

Dane konta użytkownika

Dane niezbędne do prowadzenia konta, w szczególności imię, nazwisko, adres e-mail i informacje związane z kontem, są przechowywane przez okres posiadania aktywnego konta przez użytkownika.

Po usunięciu konta dane są usuwane lub anonimizowane, z wyjątkiem informacji, których dalsze przechowywanie jest wymagane przez prawo albo konieczne do dochodzenia lub obrony roszczeń.

Dane dotyczące subskrypcji

Informacje dotyczące statusu subskrypcji są przechowywane przez okres trwania subskrypcji oraz przez okres niezbędny do rozliczenia zakończonej usługi.

Dane dotyczące płatności i dokumentacji rozliczeniowej

Dane, których zachowanie jest wymagane na podstawie przepisów podatkowych lub rachunkowych, są przechowywane przez okres wynikający z właściwych przepisów prawa.

W przypadkach, w których zastosowanie ma pięcioletni okres przechowywania dokumentacji lub przedawnienia zobowiązań podatkowych, okres ten jest obliczany zgodnie z właściwymi przepisami podatkowymi i rachunkowymi.

DANGER STUDIO nie przechowuje pełnych danych kart płatniczych. Pełne dane instrumentów płatniczych obsługują właściwi dostawcy płatności.

Dane dotyczące postępów i rankingu

Dane przechowywane w Supabase, w szczególności nick, ranking oraz postępy użytkownika, są przechowywane przez okres posiadania konta i korzystania z usługi.

Po usunięciu konta dane przypisane do użytkownika są usuwane lub anonimizowane, chyba że dalsze ich przechowywanie jest wymagane przez przepisy prawa.

Statystyki korzystania z Aplikacji

Opcjonalne statystyki służą porównywaniu własnych ćwiczeń oraz analizie popularności funkcji i zbiorczych wyników ćwiczeń w celu rozwijania Danger Studio. Szczegółowe zdarzenia aktywności są przechowywane przez 24 miesiące kalendarzowe, chyba że wcześniej zostaną usunięte. Podczas okresowego porządkowania starsze zdarzenia są zastępowane skumulowanymi podsumowaniami liczbowymi kategorii ćwiczeń i narzędzi.

Osobiste podsumowania pozostają powiązane z kontem do wycofania zgody, usunięcia historii lub konta. Nie zawierają dawnych dat aktywności, identyfikatorów zdarzeń i sesji ani nazw prywatnych plików lub presetów. Są nadal danymi powiązanymi z użytkownikiem.

Widok całej historii łączy bieżące dane szczegółowe ze starszymi podsumowaniami kategorii. Średnie i skuteczność obliczane są z zachowanych sum i liczników; rekordy zachowują wartości maksymalne lub minimalne. Wykresy, daty, serie aktywności i ulubione ustawienia odnoszą się do dostępnej historii szczegółowej z ostatnich 24 miesięcy.

Pauza nowych zapisów pozostawia zgodę na przechowywanie i podsumowywanie historii aktywną; nie zatrzymuje okresowego zastępowania starszych zdarzeń podsumowaniami. Wycofanie zgody przez „Wycofaj zgodę i usuń statystyki”, usunięcie historii lub konta obejmuje wszystkie osobiste warstwy statystyk. Usuwane dane nie są najpierw przenoszone do globalnych sum.

Usunięcie historii statystyk lub konta i wycofanie zgody nie pomniejsza już zgromadzonych niezależnych globalnych podsumowań, które nie zawierają zapisanej mapy wkładu poszczególnych kont. Globalne sumy przechowujemy przez okres prowadzenia i rozwijania Danger Studio. Co najmniej raz w roku sprawdzamy, czy ich zakres i dalsze przechowywanie są nadal potrzebne.

Historia czatu AI

Historia rozmów widoczna w Danger Studio App jest przechowywana lokalnie na komputerze użytkownika do czasu jej usunięcia przez użytkownika.

Użytkownik może usunąć historię z poziomu Aplikacji lub poprzez usunięcie odpowiednich lokalnych plików.

Treści przekazywane przez OpenAI API mogą być czasowo przechowywane przez dostawcę dla bezpieczeństwa i przeciwdziałania nadużyciom, mimo wyłączenia zapisywania odpowiedzi jako przechowywanego zasobu API. Zasady opisano w rozdziale 11.

Dane audio

Dźwięk analizowany przez system weryfikacji ćwiczeń nie jest archiwizowany ani przechowywany przez DANGER STUDIO po zakończeniu bieżącej analizy.

Potwierdzenia usuwania konta

Kod potwierdzający jest ważny przez 10 minut. W bazie przechowujemy jego zabezpieczone potwierdzenie, nie jawną treść. Niezatwierdzone żądania są porządkowane po 24 godzinach od ostatniego wygenerowania kodu.

Przez 30 dni od zakończenia przechowujemy ograniczone techniczne potwierdzenie realizacji: pseudonimowe oznaczenie, skróty tokenów, czasy i stan operacji oraz niezbędne dane techniczne, bez jawnego identyfikatora członka i kontaktu Wix. Następnie jest usuwane w cyklu porządkowania. Niezakończone żądania pozostają do rozpatrzenia, także gdy wymagają ręcznej interwencji.

Link do statusu realizacji działa przez 30 dni od potwierdzenia żądania. Jest to termin odrębny od okresu przechowywania technicznego potwierdzenia zakończenia operacji.

Kopie zapasowe

Usunięcie danych w systemie bieżącym nie oznacza natychmiastowego usunięcia wszystkich kopii zapasowych. Kopie zapasowe podlegają odrębnym cyklom retencji stosowanym w wykorzystywanych usługach dostawców.

Rejestr wyborów cookies

Dane rejestru CookieYes są przechowywane przez okres potrzebny do udokumentowania wyborów odwiedzających, z uwzględnieniem zasady ograniczenia przechowywania wskazanej na początku tego rozdziału. Dostępność wpisów w panelu lub eksporcie nie jest równoznaczna z terminem usunięcia wszystkich kopii. Terminy usuwania danych po zakończeniu umowy z CookieYes nie określają bieżącej retencji rejestru podczas korzystania z usługi.

Dane związane z roszczeniami

Jeżeli jest to konieczne do ustalenia, dochodzenia lub obrony roszczeń, określone dane mogą być przechowywane do czasu upływu właściwego okresu przedawnienia.

Po ustaniu celu przetwarzania oraz okresów wymaganych prawem dane są usuwane lub trwale anonimizowane.

21. Usunięcie konta

Usunięcie konta można zlecić na stronie https://www.dangerstudioapp.com/usun-konto. Samo otwarcie strony ani wysłanie kodu nie usuwa konta. Potwierdzenie wymaga zalogowania, kodu wysłanego na adres e-mail konta oraz potwierdzenia skutków operacji. Po przyjęciu potwierdzonego żądania unieważniamy sesje Aplikacji. W toku realizacji kończymy powiązane plany cenowe, usuwamy członkostwo i kontakt Wix oraz konto i powiązane dane Aplikacji w Supabase, w tym historię i osobiste sumy statystyk, postęp lekcji, wyniki i odblokowania gry.

Przyjęcie żądania nie oznacza zakończenia wszystkich czynności. Przed rozpoczęciem usuwania wysyłamy wiadomość o przyjęciu żądania z linkiem do statusu realizacji. Link działa bez logowania przez 30 dni od potwierdzenia żądania i służy wyłącznie do odczytu statusu. Zakończenie jest pokazywane po potwierdzeniu czynności w Wix i Supabase. Link należy zachować i nie udostępniać go innym.

Usunięcie konta nie usuwa automatycznie wszystkich plików na komputerze użytkownika. Lokalna historia czatu, własne pliki, ustawienia i pamięć podręczna mogą wymagać samodzielnego usunięcia. Dokumentacja rozliczeniowa oraz kopie zapasowe podlegają odrębnym zasadom retencji opisanym w rozdziale 20.

Określone informacje dotyczące płatności, dokumentacji księgowej lub transakcji mogą być przechowywane przez DANGER STUDIO, Wix, Stripe, PayPal lub innych właściwych dostawców przez okres wynikający z obowiązujących przepisów prawa lub ich własnych obowiązków prawnych. Usunięcie konta Danger Studio nie zamyka konta PayPal ani portfela użytkownika i nie usuwa automatycznie wszystkich zapisów operatorów płatności.

Po wygaśnięciu linku do statusu lub w razie problemów z usunięciem konta można skontaktować się z DANGER STUDIO pod adresem dangerstudio.app@gmail.com. Ten adres służy również do zgłaszania żądań dotyczących danych poza formularzem samoobsługowym.

22. Prawa użytkownika

Na zasadach określonych w RODO użytkownikowi mogą przysługiwać następujące prawa:

- Prawo dostępu do danych.
- Prawo uzyskania kopii danych.
- Prawo do sprostowania danych.
- Prawo do usunięcia danych.
- Prawo do ograniczenia przetwarzania.
- Prawo do przenoszenia danych.
- Prawo do wniesienia sprzeciwu wobec przetwarzania.
- Prawo do wycofania zgody, jeżeli przetwarzanie odbywa się na jej podstawie.

Zakres poszczególnych praw zależy od podstawy prawnej i okoliczności przetwarzania.

W celu skorzystania ze swoich praw użytkownik może skontaktować się z: **dangerstudio.app@gmail.com**.

Użytkownik może również zwrócić się o usunięcie określonych danych związanych z jego kontem, w tym danych dotyczących aktywności lub statystyk, bez konieczności składania żądania usunięcia całego konta, o ile zachowanie takich danych nie jest wymagane na podstawie obowiązujących przepisów lub innej właściwej podstawy prawnej.

DANGER STUDIO może poprosić o informacje pozwalające zweryfikować tożsamość osoby składającej żądanie, jeżeli będzie to konieczne do ochrony danych użytkownika.

23. Prawo do wniesienia skargi

Użytkownik ma prawo złożyć skargę do organu nadzorczego właściwego w sprawach ochrony danych osobowych. W Polsce organem tym jest:

Prezes Urzędu Ochrony Danych Osobowych (PUODO).

Prawo do wniesienia skargi nie ogranicza możliwości wcześniejszego skontaktowania się z DANGER STUDIO w celu wyjaśnienia problemu.

24. Wiek użytkowników

Usługa jest przeznaczona wyłącznie dla osób, które ukończyły 18 lat. Przy rejestracji wymagamy oświadczenia o pełnoletności i zapoznaniu się z Regulaminem. Przy rejestracji przez Google lub Facebook oświadczenie następuje w dodatkowym kroku po uwierzytelnieniu u dostawcy, przed zalogowaniem do witryny. Oświadczenie nie jest weryfikacją dokumentu tożsamości.

W sprawach dotyczących wieku użytkowników i ich danych można skontaktować się z DANGER STUDIO pod adresem dangerstudio.app@gmail.com.

25. Bezpieczeństwo danych

DANGER STUDIO stosuje odpowiednie środki techniczne i organizacyjne mające na celu ochronę danych przed:

- Nieuprawnionym dostępem.
- Utratą.
- Zniszczeniem.
- Zmianą.
- Ujawnieniem.
- Niewłaściwym wykorzystaniem.

Dostęp do danych użytkowników jest ograniczony do zakresu niezbędnego do świadczenia usług. Istotna część danych związanych z Danger Studio App jest przechowywana lokalnie na urządzeniu użytkownika. Bezpieczeństwo danych lokalnych zależy również od bezpieczeństwa urządzenia użytkownika, jego systemu Windows, konta systemowego oraz stosowanych przez niego zabezpieczeń.

Użytkownik powinien w szczególności:

- Chronić hasło do swojego konta.
- Nie udostępniać danych logowania osobom trzecim.
- Zabezpieczać komputer przed nieuprawnionym dostępem.
- Korzystać z aktualnego oprogramowania i zabezpieczeń systemu.

26. Brak sprzedaży danych

DANGER STUDIO nie sprzedaje danych osobowych użytkowników. Dane nie są przekazywane reklamodawcom w celu umożliwienia im prowadzenia reklamy behawioralnej lub tworzenia profili reklamowych użytkowników.

Dane są przekazywane podmiotom trzecim wyłącznie w zakresie koniecznym do zapewnienia działania usług, realizacji umowy, przetwarzania płatności, świadczenia funkcji Aplikacji lub wykonania obowiązków prawnych.

27. Zautomatyzowane podejmowanie decyzji

DANGER STUDIO nie wykorzystuje danych osobowych użytkowników do podejmowania decyzji wywołujących wobec nich skutki prawne wyłącznie na podstawie zautomatyzowanego przetwarzania danych w rozumieniu **art. 22 RODO**.

Automatyczne sprawdzanie statusu subskrypcji służy jedynie technicznej weryfikacji prawa użytkownika do korzystania z opłaconej usługi. Autorski system analizy dźwięku służy wyłącznie do oceny poprawności

wykonywanego ćwiczenia muzycznego i nie jest wykorzystywany do podejmowania decyzji prawnych dotyczących użytkownika.

28. Dostępność terytorialna

Danger Studio App i usługi DANGER STUDIO są obecnie przeznaczone dla użytkowników na terytorium **Polski**.

Polityka Prywatności została przygotowana przede wszystkim z uwzględnieniem przepisów prawa polskiego oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, czyli RODO.

29. Zmiany Polityki Prywatności

DANGER STUDIO może okresowo aktualizować niniejszą Politykę Prywatności. Zmiany mogą wynikać między innymi z:

- Rozwoju Danger Studio App.
- Dodania nowych funkcji.
- Zmiany sposobu przetwarzania danych.
- Zmiany wykorzystywanych usług zewnętrznych.
- Zmian przepisów prawa.
- Zmian wymogów dotyczących bezpieczeństwa.

Aktualna wersja Polityki Prywatności będzie publikowana na stronie: **https://www.dangerstudioapp.com/**.

W przypadku istotnych zmian DANGER STUDIO może poinformować użytkowników w odpowiedni sposób, w szczególności za pomocą strony internetowej lub komunikatu w aplikacji.

30. Zewnętrzni dostawcy usług

DANGER STUDIO korzysta z usług zewnętrznych dostawców technologii niezbędnych do działania strony internetowej oraz Danger Studio App.

Do głównych dostawców należą:

Dostawca	Zakres / rola
Wix.com	Strona internetowa, konta użytkowników i logowanie.
Render	Infrastruktura backendowa wykorzystywana przez Danger Studio App.
Stripe i PayPal	Płatności i subskrypcje zależnie od wybranej metody; Apple Pay i Google Pay są obsługiwane przez Stripe.
Supabase	Dane konta i funkcji Aplikacji, w tym postęp lekcji i ranking oraz, po wyrażeniu zgody, opcjonalne statystyki aktywności i osobiste podsumowania kategorii.
Cloudflare R2	Przechowywanie i dostarczanie instalatorów oraz filmów lekcji; dane techniczne żądań pobrania.
OpenAI	Funkcja czatu AI.
Google	Opcjonalne logowanie przez Google i ochrona formularza rejestracyjnego przez reCAPTCHA.

Dostawca	Zakres / rola
Meta Platforms / Facebook	Opcjonalne logowanie za pomocą konta Facebook.
CookieYes Limited	Zarządzanie preferencjami cookies i rejestr wyborów odwiedzających, w naszym imieniu.

Dostawcy ci posiadają własne polityki prywatności określające szczegółowe zasady przetwarzania przez nich danych. DANGER STUDIO zaleca zapoznanie się z tymi dokumentami w przypadku korzystania z funkcji opartych na usługach danego dostawcy.

W zależności od charakteru konkretnego procesu dostawca może działać jako:

- Podmiot przetwarzający dane w imieniu DANGER STUDIO.
- Dalszy podmiot przetwarzający.
- Niezależny administrator danych.
- Albo pełnić różne role w odniesieniu do różnych kategorii danych.

W przypadku, gdy dostawca przetwarza dane osobowe w imieniu DANGER STUDIO jako podmiot przetwarzający, współpraca odbywa się zgodnie z wymaganiami art. 28 RODO, na podstawie odpowiednich warunków umownych lub umowy dotyczącej przetwarzania danych.

Do głównych dostawców należą:

Wix

Wix zapewnia infrastrukturę witryny, obsługę kont użytkowników, rejestracji i logowania, subskrypcji oraz wiadomości obsługowych.

Zgodnie ze standardowymi warunkami i umową powierzenia Wix usługę zapewnia Wix.com Ltd. wraz ze spółkami grupy. W zakresie danych użytkowników przetwarzanych w naszym imieniu zastosowanie ma umowa powierzenia: https://www.wix.com/about/privacy-dpa-users. Wix może również realizować własne cele przetwarzania zgodnie ze swoimi warunkami i polityką prywatności.

Render

Render zapewnia infrastrukturę backendu Aplikacji w regionie Frankfurt w Niemczech. Zgodnie ze standardowymi warunkami dostawcą jest Render Services, Inc. (USA). Dla danych przetwarzanych na nasze zlecenie działa jako podmiot przetwarzający na podstawie umowy powierzenia: https://render.com/dpa.

Stripe i PayPal

Płatności obsługuje Stripe lub PayPal, zależnie od wybranej metody. Apple Pay i Google Pay są w naszej konfiguracji obsługiwane przez Stripe. Zgodnie ze standardowymi warunkami dla Polski podmiotami Stripe są Stripe Payments Europe, Limited i Stripe Technology Europe, Limited, a podmiotem PayPal jest PayPal (Europe) S.à r.l. et Cie, S.C.A. z siedzibą w Luksemburgu. Dokumenty Stripe: https://stripe.com/legal/ssa/pl oraz https://stripe.com/legal/dpa. Polityka prywatności PayPal: https://www.paypal.com/pl/legalhub/paypal/privacy-full.

W zależności od rodzaju wykonywanej operacji Stripe może działać jako podmiot przetwarzający dane w imieniu DANGER STUDIO albo jako niezależny administrator danych, w szczególności w zakresie realizacji własnych obowiązków prawnych, bezpieczeństwa płatności i przeciwdziałania oszustwom.

PayPal realizuje również własne cele płatnicze, bezpieczeństwa i obowiązki prawne jako odrębny administrator; jego wszystkich operacji nie należy utożsamiać z przetwarzaniem w imieniu DANGER STUDIO.

Supabase

Supabase zapewnia infrastrukturę wykorzystywaną do przechowywania i obsługi wybranych danych związanych z kontem użytkownika, subskrypcją, sesjami, postępami, rankingiem oraz innymi funkcjami Danger Studio App.

Zgodnie ze standardowymi warunkami dostawcą jest Supabase Pte. Ltd. (Singapur). Podstawowy projekt bazy danych działa w regionie Irlandia (eu-west-1). Dane przetwarzane na nasze zlecenie podlegają umowie powierzenia: https://supabase.com/legal/customer-resources/data-processing-addendum. Lokalizacja projektu nie oznacza ograniczenia wszystkich operacji wsparcia, obsługi konta i infrastruktury globalnej do tego regionu.

Cloudflare

Cloudflare R2 służy do przechowywania i dostarczania instalatorów oraz filmów lekcji. Podczas pobierania Cloudflare może technicznie przetwarzać dane żądania, w tym adres IP użytkownika. W konfiguracji obu używanych zasobów wskazano preferowaną lokalizację Eastern Europe (EEUR). To ustawienie nie gwarantuje przechowywania wszystkich danych w tym obszarze ani ograniczenia wszystkich operacji do UE. Zgodnie ze standardowymi warunkami dostawcą jest Cloudflare, Inc. (USA). Powierzenie i zabezpieczenia właściwych transferów określa umowa: https://www.cloudflare.com/cloudflare-customer-dpa/.

OpenAI

OpenAI zapewnia usługę API wykorzystywaną przez funkcję czatu AI.

Zgodnie ze standardowymi warunkami dla klientów z Polski stroną umowy jest OpenAI Ireland Ltd. W zakresie danych przetwarzanych w naszym imieniu zastosowanie ma umowa powierzenia: https://openai.com/policies/data-processing-addendum/. Irlandzka siedziba podmiotu umowy nie oznacza europejskiej rezydencji projektu API. Zakres przekazywanej treści i przetwarzania dla bezpieczeństwa opisano w rozdziale 11.

Google i Meta / Facebook

Google oraz Meta mogą przetwarzać dane użytkownika w związku z wybraniem przez niego odpowiedniego sposobu logowania.

Zakres oraz rola tych podmiotów zależą od wykorzystywanego mechanizmu logowania i ich własnych warunków świadczenia usług.

Google reCAPTCHA jest również wykorzystywana do ochrony formularza rejestracyjnego przed botami. Zasady przetwarzania opisują dokumenty Google: https://policies.google.com/privacy?hl=pl. Rola dostawcy zależy od wykorzystywanej usługi i danej operacji.

CookieYes

CookieYes Limited (Wielka Brytania) dostarcza narzędzie zarządzania preferencjami cookies i rejestrowania wyborów odwiedzających. Dane te przetwarza w naszym imieniu. Zgodnie ze standardowymi warunkami dostawcy zasady powierzenia i zabezpieczenia transferów określa umowa: https://www.cookieyes.com/dpa/. Polityka prywatności CookieYes opisująca także własne operacje dostawcy jest dostępna pod adresem https://www.cookieyes.com/privacy-policy/.

DANGER STUDIO dobiera dostawców z uwzględnieniem odpowiednich gwarancji dotyczących bezpieczeństwa i ochrony danych osobowych oraz okresowo może aktualizować listę wykorzystywanych dostawców.

W zależności od charakteru świadczonej usługi poszczególni dostawcy mogą przetwarzać dane w imieniu DANGER STUDIO albo realizować własne obowiązki związane z funkcjonowaniem świadczonych przez nich usług.

W przypadku, gdy dostawca przetwarza dane osobowe w imieniu DANGER STUDIO, współpraca odbywa się zgodnie z wymaganiami obowiązujących przepisów dotyczących ochrony danych osobowych.

Poszczególni dostawcy posiadają własne polityki prywatności i zasady dotyczące ochrony danych, określające szczegółowe warunki przetwarzania informacji w ramach ich usług.

31. Kontakt

Wszelkie pytania dotyczące:

- Polityki Prywatności.
- Danych osobowych.
- Usunięcia danych.
- Usunięcia konta.
- Realizacji praw wynikających z RODO.
- Bezpieczeństwa danych.

można kierować do:

DANGER STUDIO, Polska

E-mail: dangerstudio.app@gmail.com

Strona internetowa: https://www.dangerstudioapp.com/

32. Podsumowanie sposobu przetwarzania danych

W ramach usług DANGER STUDIO wykorzystywane są następujące główne systemy i dostawcy:

Dostawca	Zakres / rola
Wix	Zapewnia infrastrukturę strony internetowej, kont użytkowników, rejestrację, logowanie oraz obsługę informacji związanych z subskrypcją.
Render	Zapewnia infrastrukturę backendu Danger Studio App i technicznie pośredniczy w komunikacji pomiędzy Aplikacją a innymi usługami.
Stripe i PayPal	Obsługują płatności zależnie od wybranej metody. Apple Pay i Google Pay są obsługiwane przez Stripe. DANGER STUDIO nie przechowuje pełnych danych kart płatniczych.
Supabase	Przechowuje dane konta, subskrypcji, sesji, postępu lekcji i rankingu oraz, po wyrażeniu zgody, szczegółowe statystyki aktywności i osobiste podsumowania kategorii. Treść rozmów AI nie jest w nim zapisywana.
Cloudflare R2	Przechowuje i dostarcza instalatory oraz filmy lekcji. Podczas pobierania przetwarzane są dane techniczne żądań.
OpenAI API	Przetwarza bieżące pytanie i instrukcję systemową do wygenerowania odpowiedzi oraz dla bezpieczeństwa i przeciwdziałania nadużyciom zgodnie z zasadami usługi API. Komunikacja odbywa się przez backend Danger Studio App.
Google i Meta lub Facebook	Uczestniczą w logowaniu, jeśli użytkownik wybierze odpowiednią metodę. Google reCAPTCHA dodatkowo chroni formularz rejestracyjny przed botami.
Komputer użytkownika	Przechowuje lokalną historię rozmów AI, określone dane Aplikacji oraz tymczasową kolejkę niewysłanych zdarzeń statystycznych wykorzystywaną w przypadku braku połączenia z usługą.

Dostawca	Zakres / rola
Autorski system analizy dźwięku	Analizuje dźwięk na bieżąco podczas wykonywania ćwiczenia, bez jego archiwizowania przez DANGER STUDIO.
CookieYes Limited	Zapewnia panel preferencji cookies i rejestr wyborów odwiedzających. Ustawienia cookies strony są odrębne od zgody na statystyki Aplikacji.

DANGER STUDIO nie wykorzystuje danych użytkowników do reklam, nie sprzedaje danych osobowych i nie przechowuje pełnych danych kart płatniczych.