

[• DOKUMENTY](#)

Umowa powierzenia przetwarzania

Ta umowa dotyczy jedynego przypadku, w którym faktycznie przetwarzamy dane osobowe w Twoim imieniu: zamrożonej aplikacji webowej pod adresem `app.sumizai.com`. **Aplikacja desktopowa nie wysyła nam niczego** — ani konta, ani notatki, ani pytania, ani klucza — więc nie ma tam powierzenia, które ta umowa miałaby regulować. Przeczytaj pierwszą sekcję, zanim poprosisz nas o podpis.

Ostatnia aktualizacja: 2026-08-14 Wersja: 1.0

Operator: 10UP Jan Śliwa, Kminkowa 26, 72-003 Bezrzecze, Polska

01 Kiedy ta umowa obowiązuje (a kiedy nie)

SumizAI to nazwa trzech różnych rzeczy. Tylko jedna z nich stawia nas w roli podmiotu przetwarzającego. To jest ważniejsze niż wszystko inne w tym dokumencie, więc stoi na początku.

Aplikacja desktopowa — ta umowa nie obowiązuje

Aplikacja desktopowa nie ma kont, logowania ani żadnego naszego serwera. Baza danych leży w `~/Library/Application Support/app.sumizai.desktop/sumizai.db`, notatki to pliki `.md` w wybranym przez Ciebie folderze, a klucz do dostawcy AI siedzi w pęku kluczy systemu operacyjnego. Zapytania do dostawcy AI idą prosto z Twojego urządzenia do wybranego przez Ciebie dostawcy; nie przechodzą przez żaden serwer SumizAI. Nie ma telemetry, analityki, raportowania awarii ani automatycznych aktualizacji. Nie otrzymujemy więc żadnych Twoich danych osobowych i żadnych nie przetwarzamy. Podpisanie umowy powierzenia dla produktu desktopowego opisywałoby relację, która nie istnieje.

Strona `sumizai.com` — ta umowa nie obowiązuje

Na stronie marketingowej działają Google Analytics 4 i Microsoft Clarity, i to wyłącznie po wyrażeniu zgody. Tam jesteśmy *administratorem*, a nie Twoim procesorem, więc relację opisuje [Polityka prywatności](#) i [Polityka cookies](#), a nie ta umowa.

Aplikacja webowa `app.sumizai.com` — ta umowa obowiązuje

Starsza aplikacja webowa trzyma konta w bazie danych, a pliki notatek w magazynie obiektowym na serwerze, który prowadzimy, i wywołuje dostawcę AI w Twoim imieniu przy

użyciu podanego przez Ciebie klucza. To jest przetwarzanie danych osobowych na Twoje polecenie. Wszystko poniżej dotyczy tej aplikacji i niczego więcej.

Aplikacja webowa jest zamrożona: to nie jest produkt, który rozwijamy. Ten dokument nie twierdzi, że instancja jest obecnie wdrożona i otwarta dla użytkowników — jeśli nie masz tam konta, ta umowa nie ma przedmiotu i nie jest Ci potrzebna.

02 Definicje i pierwszeństwo

- **RODO** — rozporządzenie (UE) 2016/679.
- **Operator, my** — 10UP Jan Śliwa, Kminkowa 26, 72-003 Bezrzecze, Polska, NIP 8521091009, kontakt contact@sumizai.com.
- **Klient, Ty** — osoba lub organizacja posiadająca konto w aplikacji webowej i wydająca nam polecenia przez korzystanie z niej.
- **Aplikacja webowa** — oprogramowanie serwowane pod adresem app.sumizai.com.
- **Treść Klienta** — notatki, źródłowe pytania i odpowiedzi, rozmowy i struktura sejfów tworzone w aplikacji webowej wraz z danymi osobowymi, które zdecydujesz się w nich umieścić.
- **Podprocesor** — podmiot trzeci, któremu powierzamy przetwarzanie danych objętych tą umową *w naszym imieniu*. Wykaz znajduje się w pierwszej tabeli Załącznika 3; druga tabela tego załącznika wymienia podmioty, które podprocesorami wyraźnie nie są.

Ta umowa stanowi część [Regulaminu](#). Jeśli oba dokumenty mówią co innego w kwestii ochrony danych, pierwszeństwo ma ta umowa. Jeśli ta umowa i RODO wydają się mówić co innego, pierwszeństwo ma RODO, a sprzeczne zdanie należy czytać jako nieistniejące, a nie jako wymówkę.

03 Role stron

Ty jesteś administratorem danych konta i Treści Klienta w aplikacji webowej. To Ty decydujesz, co trafia do notatki. **My jesteśmy podmiotem przetwarzającym** i działamy na Twoje udokumentowane polecenie.

Jeśli sam jesteś procesorem dla kogoś innego, powierzasz nam dane jako podprocesorowi, a tę umowę czyta się wtedy o jedno ogniwo dalej w łańcuchu. Potwierdzasz w takim przypadku, że masz do tego upoważnienie.

Za co odpowiadasz Ty

Jako administrator decydujesz, po co i w jaki sposób dane są przetwarzane, i ta część zostaje po Twojej stronie. W szczególności odpowiadasz za podstawę prawną dla danych osobowych, które umieszczasz w aplikacji webowej, za ich prawidłowość i adekwatność, za spełnienie obowiązku informacyjnego wobec osób, których dane dotyczą, i za odpowiadanie na ich żądania, a także za

ewentualne zgłoszenie naruszenia organowi nadzorczemu i zawiadomienie osób. Ponieważ środki z Załącznika 2 nie są pod to projektowane, nie powinieneś wprowadzać do aplikacji danych szczególnych kategorii (art. 9 RODO) ani danych o wyrokach skazujących (art. 10). To Ty wybierasz też dostawcę AI, a wybierając go decydujesz, że Twoja treść może być do niego wysłana.

Występujemy jako **odrębny administrator**, a nie jako Twój procesor, w wąskim zakresie własnych celów: korespondencja, którą wysyłasz na contact@sumizai.com, oraz dokumentacja, którą musimy przechowywać na podstawie polskich przepisów rachunkowych i podatkowych. Ta skrzynka jest nasza własna: działa na naszym serwerze w Niemczech (Postfix i Dovecot), więc tego, co do nas piszesz, nie przechowuje żaden dostawca poczty. Logi serwera prowadzimy jednocześnie w ramach świadczenia usługi dla Ciebie i dla własnego bezpieczeństwa, więc traktujemy je w ramach tej umowy i postępujemy z nimi tak, jak opisuje [Polityka prywatności](#).

Dostawca AI to Twoja relacja, nie nasza. Aplikacja nie ma własnego dostępu do AI — wybierasz jednego z obsługiwanych dostawców i podajesz własny klucz. Kiedy aplikacja webowa wysłała Twoją treść do tego dostawcy, robi to dlatego, że tak ją skonfigurowałeś. To, czy dostawca trenuje na tej treści, regulują warunki konta, którego klucz wkleiłeś. Nie jesteśmy stroną tamtej umowy i nie możemy jej zmienić.

04 Przedmiot, czas trwania i polecenia

Przedmiot. Hosting i prowadzenie aplikacji webowej: przechowywanie rekordu konta i sejfów, ich indeksowanie oraz przekazywanie Twojej treści wybranemu przez Ciebie dostawcy AI, aby aplikacja mogła zredagować notatkę, umieścić ją w spisie treści i sprawdzić, czy nie powtarza istniejącej.

Czas trwania. Tak długo, jak masz konto i jak przechowujemy Twoje dane, a potem tylko przez krótki czas potrzebny na wykonanie usunięcia albo eksportu, o który poprosisz, lub przez okres, w którym przepis nakazuje nam zachować konkretny dokument.

Polecenia. Twoje udokumentowane polecenia to: ta umowa, [Regulamin](#), ustawienia, które konfigurujesz w aplikacji (w tym wybór dostawcy AI), oraz wszystko, co prześlesz nam pisemnie na contact@sumizai.com. Przetwarzamy dane osobowe wyłącznie na tych poleceniach, w tym w zakresie przekazywania do państw trzecich, chyba że wymaga tego prawo UE lub prawo polskie — wtedy informujemy Cię przed przetwarzaniem, o ile ten sam przepis nie zabrania takiej informacji.

Jeżeli uznamy, że polecenie narusza RODO lub polskie przepisy o ochronie danych, mówimy o tym wprost i możemy wstrzymać wykonanie tego polecenia do czasu wyjaśnienia.

Pełne kategorie osób i danych opisuje Załącznik 1.

05 Nasze obowiązki jako procesora

Poufność

Każda osoba upoważniona do przetwarzania danych na podstawie tej umowy jest zobowiązana do zachowania poufności — umownie albo z mocy ustawy. Jesteśmy jednoosobową działalnością gospodarczą, więc krąg osób z dostępem jest z natury wąski, a dostęp ograniczamy do tego, co jest potrzebne do prowadzenia i wsparcia usługi.

Bezpieczeństwo

Stosujemy środki techniczne i organizacyjne wymienione w **Załączniku 2**. Ten załącznik wymienia to, co faktycznie istnieje w kodzie, i mówi też wprost, czego nie ma — przede wszystkim, że **nie istnieją automatyczne kopie zapasowe**. Przeczytaj go, zanim zdecydujesz, co trzymać w aplikacji webowej.

Pomoc przy żądaniach osób, których dane dotyczą

Pomagamy Ci odpowiadać na żądania z art. 15–22 RODO, biorąc pod uwagę charakter przetwarzania. W praktyce:

- **Dostęp i przenoszenie** — aplikacja eksportuje sejf do pliku ZIP, a także do PDF i PowerPointa. Pola konta podajemy na żądanie.
- **Usunięcie** — aplikacja webowa nie ma samoobsługowego punktu usuwania konta. Schemat bazy poprawnie kaskaduje usunięcie, ale uruchamia je wyłącznie ręczna operacja. Napisz na contact@sumizai.com, wykonamy usunięcie i potwierdzimy je pisemnie.
- **Sprostowanie i ograniczenie** — również obsługiwane ręcznie, na pisemne żądanie.
- Produkt nie wysyła żadnych wiadomości e-mail: nie ma w nim wysyłki poczty w ogóle, nie ma maila weryfikacyjnego ani resetu hasła. Wszystko tego rodzaju idzie przez contact@sumizai.com, od człowieka.

Pomoc przy art. 32–36

Pomagamy Ci — uwzględniając charakter przetwarzania i informacje, którymi dysponujemy — w zapewnieniu bezpieczeństwa przetwarzania, w zgłaszaniu naruszeń i zawiadamianiu osób, w ocenie skutków dla ochrony danych oraz w uprzednich konsultacjach z organem nadzorczym. Konkretnie oznacza to pisemne odpowiedzi na Twoje pytania i udostępnienie faktów z Załącznika 1 i 2. Nie mamy raportu z audytu ani certyfikatu, którym moglibyśmy zastąpić tę odpowiedź.

Rejestr

Prowadzimy rejestr kategorii czynności przetwarzania dokonywanych w Twoim imieniu, zgodnie z art. 30 ust. 2 RODO, i udostępniamy go Tobie lub organowi nadzorczemu na żądanie.

Usunięcie albo zwrot

Po zakończeniu przetwarzania wybierasz usunięcie albo zwrot danych; szczegóły w sekcji o czasie trwania i rozwiązaniu umowy.

06 Podprocesorzy

Udzielasz **ogólnej pisemnej zgody** na korzystanie przez nas z podprocesorów wymienionych w pierwszej tabeli **Załącznika 3**, na warunkach z tej sekcji.

Przeczytaj ten załącznik uważnie, bo wymienia też podmioty, które **nie są** naszymi podprocesorami: logowanie przez Google, logowanie przez Apple i wybranego przez Ciebie dostawcę AI. Nie powierzamy im danych w Twoim imieniu — dostawcy logowania działają na własny rachunek, gdy użytkownik wybierze tę drogę, a dostawca AI to relacja między Tobą a nim, otwarta kluczem, który podałeś. Zobowiązania z tej sekcji, w tym nasza pełna odpowiedzialność za podprocesora, dotyczą podprocesorów, którym my powierzamy dane; nie możemy uczciwie rozciągać ich na podmioty, których warunków ani nie ustalamy, ani nie podpisujemy.

- Każdego podprocesora wiążą obowiązki ochrony danych nie słabsze niż te z tej umowy.
- Pozostajemy wobec Ciebie **w pełni odpowiedzialni** za wykonanie tych obowiązków przez podprocesora.
- Przed dodaniem lub zmianą podprocesora informujemy Cię z **co najmniej 30-dniowym wyprzedzeniem**. Zawiadomienie wysyła człowiek z adresu contact@sumizai.com na adres e-mail przypisany do Twojego konta, a Załącznik 3 na tej stronie dostaje nowy numer wersji i nową datę. Sam produkt nie wysyła poczty, więc nie czekaj na automatyczną wiadomość.
- W ciągu tych 30 dni możesz **zgłosić sprzeciw z uzasadnionych powodów dotyczących ochrony danych**. Spróbujemy go rozwiązać; jeśli się nie da, możesz zaprzestać korzystania z objętej zmianą części usługi i ją wypowiedzieć, a my usuniemy lub zwrócimy dane na zasadach opisanych niżej.

Załącznik 3 jest krótki. Wskazuje **Hetzner Online GmbH** z Falkenstein w Niemczech jako dostawcę maszyn, na których pracujemy, i równie wyraźnie mówi, czego nie rozstrzyga: czy zamrożona aplikacja webowa jest wdrożona właśnie na tej maszynie. Hosting tej instancji ma więc własny wiersz, wciąż bez nazwy firmy; potwierdzamy go pisemnie na żądanie, zamiast drukować tu coś, czego nie zweryfikowaliśmy. Na liście nie ma też dostawcy poczty — skrzynka stoi na naszej własnej maszynie.

07 Przekazywanie poza EOG

Infrastruktura, którą prowadzimy sami, obejmuje maszynę w chmurze Hetznera: **Hetzner Online GmbH**, Industriestrasse 25, 91710 Gunzenhausen, Niemcy, w lokalizacji **Falkenstein (FSN1)** w Niemczech. Na tej maszynie stoi strona sumizai.com i skrzynka contact@sumizai.com. Niemcy

to Unia Europejska, a więc i Europejski Obszar Gospodarczy — ten hosting nie jest więc przekazaniem do państwa trzeciego i nie wymaga dla siebie żadnego mechanizmu z rozdziału V RODO.

Nie twierdzimy tu natomiast, że działa na niej aplikacja webowa. Tego, czy ta instancja jest w ogóle wdrożona i na jakim serwerze, ten dokument nie rozstrzyga. Zapytaj pisemnie na contact@sumizai.com, a dostaniesz dostawcę, kraj i podstawę przekazania dla tej instancji, zanim się na niej oprzesz.

Zobowiązujemy się, że nie będziemy przekazywać danych objętych tą umową poza Europejski Obszar Gospodarczy ani korzystać z podprocesora, który to robi, jeżeli przekazanie nie jest objęte mechanizmem z rozdziału V RODO — decyzją o odpowiednim stopniu ochrony albo standardowymi klauzulami umownymi (decyzja wykonawcza Komisji (UE) 2021/914) wraz z dodatkowymi środkami, jeśli ocena skutków przekazania wykaże ich potrzebę.

Dwóch przekazania nie organizujemy my i nie będziemy powtarzać cudzych warunków tak, jakby były naszymi zobowiązaniami:

- **Logowanie przez Google i przez Apple** — używane tylko wtedy, gdy użytkownik wybierze tę drogę na ekranie logowania, i tylko gdy skonfigurowany jest odpowiedni identyfikator klienta. Obowiązują warunki i mechanizm przekazania danego dostawcy.
- **Wybrany przez Ciebie dostawca AI** — to Ty go wybrałeś i podałeś jego klucz, więc przekazanie następuje na warunkach Twojego konta u tego dostawcy. Jeśli używasz lokalnego Ollama pod `127.0.0.1`, nie ma żadnego przekazania: treść nie opuszcza maszyny.

08 Audyt i informacje

Na pisemne żądanie udostępniamy informacje niezbędne do wykazania zgodności z art. 28 RODO. Pytaj na contact@sumizai.com.

Nie posiadamy certyfikatu ISO 27001, SOC 2 ani porównywalnego i nie twierdzimy inaczej. Nie ma raportu z audytu strony trzeciej, który moglibyśmy przysłać zamiast odpowiedzi. Jeśli certyfikat jest dla Ciebie warunkiem koniecznym, powiedz o tym, zanim oprzesz się na aplikacji webowej.

Ty albo upoważniony przez Ciebie audytor, który nie jest naszym konkurentem i jest zobowiązany do poufności, może przeprowadzić audyt przetwarzania:

- po pisemnym zawiadomieniu z co najmniej 30-dniowym wyprzedzeniem;
- w zwykłych godzinach pracy i w sposób niezakłócający działania usługi;
- raz na 12 miesięcy, a dodatkowo po naruszeniu ochrony danych dotyczącym Ciebie lub gdy wymaga tego organ nadzorczy;

- bez dostępu do danych innych klientów, do naszych poufnych informacji wewnętrznych i do wszystkiego, czego nie możemy pokazać z uwagi na obowiązek poufności.

Koszt audytu ponosisz Ty, chyba że audyt wykaże istotne niewywiązanie się przez nas z tej umowy — wtedy własne koszty usunięcia uchybienia ponosimy my.

09 Naruszenia ochrony danych osobowych

Jeżeli stwierdzimy naruszenie ochrony danych osobowych dotyczące danych, które przetwarzamy dla Ciebie, zawiadamiamy Cię **bez zbędnej zwłoki, w każdym razie w ciągu 72 godzin** od stwierdzenia. Zawiadomienie wysyła człowiek z adresu contact@sumizai.com na adres e-mail przypisany do Twojego konta.

Zawiadomienie opisuje, w zakresie, w jakim wiemy to w danym momencie:

- charakter naruszenia, w tym kategorie i przybliżoną liczbę osób oraz wpisów, których dotyczy;
- możliwe konsekwencje;
- środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania jego skutków;
- punkt kontaktowy, pod którym można uzyskać więcej informacji.

Jeśli nie możemy podać wszystkiego naraz, przesyłamy to, co mamy, i uzupełniamy sukcesywnie, bez dalszej zbędnej zwłoki.

Zgłoszenie naruszenia organowi nadzorczemu z art. 33 i zawiadomienie osób z art. 34 to Twój obowiązek jako administratora, nie nasz. My w tym pomagamy i dostarczamy fakty, którymi dysponujemy.

Jedno uczciwe ograniczenie: logi serwera zawierają identyfikator żądania i śladu oraz maskują sekrety, ale **okres przechowywania logów nie jest jeszcze ustalony**. To, jak daleko wstecz da się odtworzyć incydent, zależy więc od tego, co jeszcze jest w logach. Podamy tu ten okres, gdy zostanie ustalony, a o stan bieżący możesz zapytać w każdej chwili.

10 Odpowiedzialność

Ta umowa nie zmienia rozkładu odpowiedzialności z [Regulaminu](#); mieści się w nim.

Art. 82 RODO stosuje się wprost: każda strona odpowiada za szkodę wyrządzoną własnym naruszeniem, procesor odpowiada, gdy działał poza zgodnymi z prawem poleceniami lub wbrew nim, a strona, która zapłaciła pełne odszkodowanie, może żądać od drugiej zwrotu jej części. Nic w tym dokumencie tego nie ogranicza ani nie wyłącza.

Nic tutaj nie ogranicza odpowiedzialności za szkodę wyrządzoną umyślnie, za szkodę na osobie ani w żadnym innym przypadku, w którym prawo polskie zakazuje ograniczenia. **Konsumenci oraz przedsiębiorcy na prawach konsumenta zachowują wszystkie uprawnienia przyznane im przez przepisy**; żadnego zdania tej umowy nie należy czytać jako odbierającego takie uprawnienie.

Ten dokument mówi, co robimy. Nie jest poradą prawną co do Twoich własnych obowiązków jako administratora.

11 Czas trwania, rozwiązanie, usunięcie albo zwrot

Ta umowa wchodzi w życie z chwilą rozpoczęcia korzystania z aplikacji webowej na warunkach Regulaminu i trwa tak długo, jak przetwarzamy dane osobowe w Twoim imieniu. Postanowienia, które ze swojej natury powinny trwać dalej — poufność, odpowiedzialność i obowiązki usunięcia danych poniżej — obowiązują po jej zakończeniu.

Po zakończeniu przetwarzania wybierasz:

1. **Zwrot** — eksportujesz seify z aplikacji do pliku ZIP, PDF lub PowerPoint, zanim konto zostanie usunięte; albo
2. **Usunięcie** — usuwamy dane. Ponieważ nie ma samoobsługowego punktu usuwania, to operacja ręczna: napisz na contact@sumizai.com, wykonamy ją i potwierdzimy pisemnie, gdy będzie zrobiona.

Dwa szczegóły, które warto znać, bo zmieniają znaczenie słowa „usunięte”:

- Pliki notatek leżą w kubeczku magazynu obiektowego z **włączonym wersjonowaniem**. Usunięcie obiektu zostawia wcześniejsze wersje, dopóki nie zostaną wyczyszczone — usunięcie na żądanie obejmuje więc także wyczyszczenie wersji usuwanych obiektów.
- Jeżeli prawo polskie nakazuje nam zachować konkretny dokument — na przykład dokumentację rachunkową i podatkową — zachowujemy tylko ten dokument, tylko przez wymagany okres i tylko w tym celu.

12 Prawo właściwe, kontakt i zmiany

Umowa podlega prawu polskiemu i bezpośrednio stosowanemu prawu Unii Europejskiej, w szczególności RODO. Nie narusza to bezwzględnie obowiązujących przepisów o ochronie konsumentów. Polskim organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych; skargę możesz złożyć do niego albo do organu w swoim kraju.

Operator i punkt kontaktowy

- 10UP Jan Śliwa, jednoosobowa działalność gospodarcza wpisana do CEIDG
- Kminkowa 26, 72-003 Bezrzecze, Polska

- NIP 8521091009
- contact@sumizai.com — wszystkie sprawy ochrony danych: sprzeciwy wobec podprocesorów, żądania usunięcia, wnioski o audyt, pytania o naruszenia

Nie wyznaczaliśmy inspektora ochrony danych i nie mamy takiego obowiązku. Nie ma osobnego adresu IOD: powyższy adres trafia do osoby, która odpowiada. Nie mamy jednostki organizacyjnej poza Unią Europejską, więc nie jest też wymagany przedstawiciel z art. 27 RODO.

Akceptacja Regulaminu jest akceptacją tej umowy w zakresie aplikacji webowej. Jeśli potrzebujesz jej jako osobnego, podpisanego dokumentu, napisz — przygotujemy go o tej samej treści.

Zmieniamy ten dokument, publikując nową wersję z nowym numerem i datą u góry strony. Zmiany obniżające poziom Twojej ochrony albo dodające podprocesora zapowiadamy z wyprzedzeniem, tak jak opisuje sekcja o podprocesorach.

13 Załącznik 1 — Opis przetwarzania

Ten załącznik opisuje przetwarzanie w aplikacji webowej pod adresem app.sumizai.com. Nie opisuje aplikacji desktopowej, w której nie przetwarzamy niczego.

POZYCJA	OPIS
Przedmiot	Prowadzenie aplikacji webowej: konta, przechowywanie sejfów i notatek oraz wywołania wybranego przez Klienta dostawcy AI.
Charakter i cel	Przechowywanie, indeksowanie, wyszukiwanie, wyświetlanie, eksport i przekazanie wybranemu przez Klienta dostawcy AI, aby powstała notatka, została umieszczona w spisie treści i sprawdzona pod kątem powtórzenia istniejącej notatki.
Czas trwania	Przez okres istnienia konta, a następnie do wykonania zgłoszonego usunięcia; dłużej tylko wtedy, gdy przepis nakazuje zachować konkretny dokument.
Kategorie osób, których dane dotyczą	Posiadacze kont i użytkownicy końcowi Klienta oraz każda osoba, o której Klient napisze w notatce, pytaniu lub rozmowie.
Kategorie danych — konto	Identyfikator, adres e-mail, skrót hasła (pusty dla kont założonych przez Google lub Apple), znaczniki czasu utworzenia i aktualizacji, język interfejsu, a dla kont OAuth nazwa dostawcy i identyfikator podmiotu u dostawcy. W schemacie nie ma kolumny na imię, awatar ani telefon.
Kategorie danych — treść	Pliki notatek w magazynie obiektowym, ich indeks w bazie, źródłowy tekst pytania i odpowiedzi, rozmowy i wiadomości, struktura sejfu i spisu treści oraz wszelkie dane osobowe, które Klient umieści w tej treści.

POZYCJA	OPIS
Dane uwierzytelniające	Klucz API Klienta do dostawcy AI, przechowywany w postaci zaszyfrowanej i odszyfrowywany po stronie serwera przy każdym żądaniu. Nigdy nie wraca do przeglądarki w pełnej postaci.
Dane techniczne	Ciasteczka sesji i CSRF; logi serwera z identyfikatorem żądania lub śladu, z maskowanymi sekretami. Okres przechowywania logów: jeszcze nieustalony — zob. sekcję o naruszeniach.
Szczegółne kategorie danych	Aplikacja o nie nie prosi i nie są jej potrzebne do działania. To Klient decyduje, co trafia do notatki; środki z Załącznika 2 nie są projektowane pod dane szczególnych kategorii, więc Klient nie powinien ich wprowadzać.
Częstotliwość	Ciągła, tak długo, jak Klient korzysta z aplikacji.
Odbiorcy	Podmioty wymienione w Załączniku 3 — nasi podprocesorzy oraz podmioty trzecie, które wchodzi do gry przez własne wybory Klienta — i nikt więcej.
Co trafia do dostawcy AI	Nie tylko wpisane pytanie. Prompt systemowy jest składany z sejf: spis treści plus pełny tekst maksymalnie pięciu najbardziej pasujących notatek, w budżecie 24 000 znaków. Aplikacja pokazuje, których notatek użyła. Pełny tekst pytania i odpowiedzi jest wysyłany ponownie, aby zredagować notatkę, umieścić ją w spisie treści i ocenić, czy nie powiela istniejącej.

14 Załącznik 2 — Środki techniczne i organizacyjne

To są środki, które istnieją w aplikacji webowej, opisane tak, jak zostały zaimplementowane. Niczego nie wpisujemy tu jako planu.

ŚRODEK	CZYM JEST NAPRAWDĘ
Przechowywane hasła	Hasła są hashowane algorytmem BCrypt, minimalna długość to osiem znaków. Konta założone przez Google lub Apple nie mają hasła w ogóle.
Klucz dostawcy w spoczynku	Klucz Klienta do dostawcy AI jest szyfrowany AES-256-GCM i odszyfrowywany po stronie serwera przy każdym żądaniu. Nigdy nie wraca do przeglądarki w pełnej postaci.
Ciasteczko sesji	<code>SUMIZAI_SESSION</code> ma flagi <code>httpOnly</code> i <code>SameSite=Lax</code> , więc skrypty strony go nie odczytują i nie jest wysyłane przy nawigacji z innych witryn.
Ochrona CSRF	Osobne ciasteczko <code>XSRF-TOKEN</code> przenosi token przeciwko fałszowaniu żądań; jest czytelne dla skryptów z założenia, bo frontend musi je odesłać przy żądaniach zmieniających stan.

ŚRODEK	CZYM JEST NAPRAWDĘ
Ograniczanie prób logowania	Pięć nieudanych prób logowania wstrzymuje konto na piętnaście minut.
Logowanie federacyjne	Logowanie przez Google i Apple działa po OIDC, a ich skrypty ładują się wyłącznie na ekranie logowania i tylko wtedy, gdy skonfigurowany jest odpowiedni identyfikator klienta.
Logi	Logi serwera zawierają identyfikator żądania i śladu oraz maskują sekrety , więc klucze i tokeny nie trafiają do nich otwartym tekstem.
Magazyn obiektowy	Pliki notatek leżą pod <code><user-id>/<vault-id>/notes/*.md</code> w kubełku z włączonym wersjonowaniem , co chroni przed przypadkowym nadpisaniem lub skasowaniem do czasu wyczyszczenia wersji.
Rozdzielenie danych	Ścieżki w magazynie i wiersze w bazie są kluczowane użytkownikiem i sejfem, więc treść jednego konta jest adresowana odrębnie od treści innego.
Wdrożenie	Aplikacja działa w kontenerach za odwrotnym proxy (Caddy).

Czego nie ma — powiedziane wprost

- **Nie istnieją automatyczne kopie zapasowe.** Wersjonowanie kubełka to nie kopia zapasowa: chroni obiekt przed nadpisaniem, a nie system przed utratą. Traktuj aplikację webową jako miejsce, w którym Twoje dane są, a nie jako jedyne miejsce, w którym są — i trzymaj własny eksport.
- Nie ma weryfikacji adresu e-mail ani resetu hasła, bo produkt nie wysyła żadnej poczty.
- Nie ma samoobsługowego usuwania konta; usunięcie to operacja ręczna na pisemne żądanie.
- **Okres przechowywania logów nie jest ustalony**, a okresu przechowywania kopii zapasowych nie ma jak podać, bo kopii nie ma.
- Nie posiadamy **żadnego certyfikatu bezpieczeństwa** — ani ISO 27001, ani SOC 2, ani równoważnego — ani żadnej oceny zgodności.

15 Załącznik 3 — Podprocesorzy

Lista jest celowo krótka i rozdziela dwie rzeczy, które często się myli: podmioty, którym *my* powierzamy przetwarzanie danych dla Ciebie, i podmioty, które wchodzą do gry przez *Twoje własne wybory*. Wykazem podprocesorów jest tylko pierwsza tabela.

Podprocesorzy, którym powierzamy dane

PODPROCESOR	CO ROBI	KIEDY UCZESTNICZY	LOKALIZACJA I PODSTAWA PRZEKAZANIA
Hetzner Online GmbH — dostawca naszej infrastruktury	Dostarcza maszyny, na których pracujemy. Industriestrasse 25, 91710 Gunzenhausen, Niemcy. Na maszynie w chmurze Hetznera, którą administrujemy sami, stoi strona sumizai.com i skrzynka contact@sumizai.com .	Stale, dla wszystkiego, co na tej maszynie działa.	Lokalizacja Falkenstein (FSN1) , Niemcy — Unia Europejska, a więc i EOG. Z tego hostingu nie wynika żadne przekazanie poza EOG, więc nie jest do niego potrzebny mechanizm z rozdziału V RODO. Nie przypisujemy Hetznerowi żadnego certyfikatu.
Dostawca hostingu zamrożonej aplikacji webowej	Prowadzi serwery i magazyn obiektowy, na których stoi ta aplikacja i leżą notatki — tam, gdzie ta instancja jest uruchomiona.	Stale, gdy ta aplikacja działa.	Niewskazany w tym dokumencie. Podajemy dostawcę, kraj i podstawę przekazania pisemnie, na żądanie wysłane na contact@sumizai.com . Wolimy zostawić ten wiersz otwarty, niż wpisać firmę, której nie potwierdziliśmy.

Dlaczego drugi wiersz jest wciąż otwarty. Pierwszy wiersz nie mówi, że na maszynie Hetznera działa zamrożona aplikacja webowa. Tego, czy ta instancja jest w ogóle wdrożona i na jakim serwerze, ten dokument nie rozstrzyga, więc jej hosting ma własny wiersz, a my zostajemy przy uczciwej odpowiedzi: napisz na contact@sumizai.com, a wskażemy dostawcę, kraj i podstawę przekazania dla tej instancji, zanim się na niej oprzesz. Niezależnie od tego obowiązuje zobowiązanie z sekcji o przekazywaniu: dane objęte tą umową nie opuszczają EOG bez mechanizmu z rozdziału V RODO.

To cały wykaz. **Nie ma dostawcy poczty:** contact@sumizai.com to skrzynka, którą prowadzimy sami (Postfix, Dovecot i OpenDKIM) na tej samej maszynie u Hetznera, więc poczta, którą do nas wysyłasz, leży na naszej własnej infrastrukturze w UE i nie trafia do żadnego procesora poza Hetznerem jako gospodarzem maszyny. Sam produkt nadal nie wysyła żadnych e-maili. W aplikacji nie ma analityki ani raportowania awarii, w kodzie nie ma operatora płatności, nie ma też usług kopii zapasowych, bo automatyczne kopie aplikacji webowej nie istnieją.

Podmioty trzecie, które nie są naszymi podprocesorami

Te podmioty otrzymują dane wskutek wyboru dokonanego po Twojej stronie, a nie dlatego, że my powierzyliśmy im coś dla Ciebie. Nie ręczymy za ich warunki, a zobowiązania z tabeli wyżej ich nie obejmują.

PODMIOT	CO ROBI	KIEDY UCZESTNICZY	CZYJA TO RELACJA
Google	Logowanie przez Google (OIDC): uwierzytelnia użytkownika i zwraca identyfikator podmiotu u dostawcy.	Tylko jeśli użytkownik wybierze tę drogę na ekranie logowania i tylko gdy skonfigurowany jest identyfikator klienta Google. Skrypt ładuje się wyłącznie na ekranie logowania.	Google działa na własny rachunek jako dostawca tożsamości. Obowiązują jego własne warunki i jego własny mechanizm przekazania; nie powtarzamy ich tutaj i za nie nie ręczymy.
Apple	Logowanie przez Apple (OIDC): uwierzytelnia użytkownika i zwraca identyfikator podmiotu u dostawcy.	Tylko jeśli użytkownik wybierze tę drogę na ekranie logowania i tylko gdy skonfigurowany jest identyfikator klienta Apple. Skrypt ładuje się wyłącznie na ekranie logowania.	Apple działa na własny rachunek jako dostawca tożsamości. Obowiązują jego własne warunki i jego własny mechanizm przekazania; nie powtarzamy ich tutaj i za nie nie ręczymy.
Dostawca AI wybrany przez Klienta	Generuje odpowiedź, tekst notatki, jej miejsce w spisie treści i ocenę powtórzenia — z treści opisanej w Załączniku 1.	Za każdym razem, gdy Klient rozpoczyna rozmowę. Klient wybiera dostawcę spośród obsługiwanych przez aplikację i podaje jego klucz; aplikacja nie ma własnego dostępu do AI. Lokalny Ollama pod 127.0.0.1 oznacza, że nic nie opuszcza maszyny.	Twoja. Klucz pochodzi z Twojego konta u tego dostawcy, więc warunki tamtego konta regulują przekazanie i to, czy dostawca trenuje na tej treści. Nie jesteśmy stroną tamtej umowy.

Nic poza tymi dwiema tabelami nie otrzymuje danych osobowych z aplikacji webowej. Strona sumizai.com ładuje po zgodzie Google Analytics 4 i Microsoft Clarity, ale to strona i nasza własna rola administratora, a nie przetwarzanie w Twoim imieniu — zob. [Politykę cookies](#). Aplikacja desktopowa nie ma żadnych podprocesorów, bo nie ma serwera.