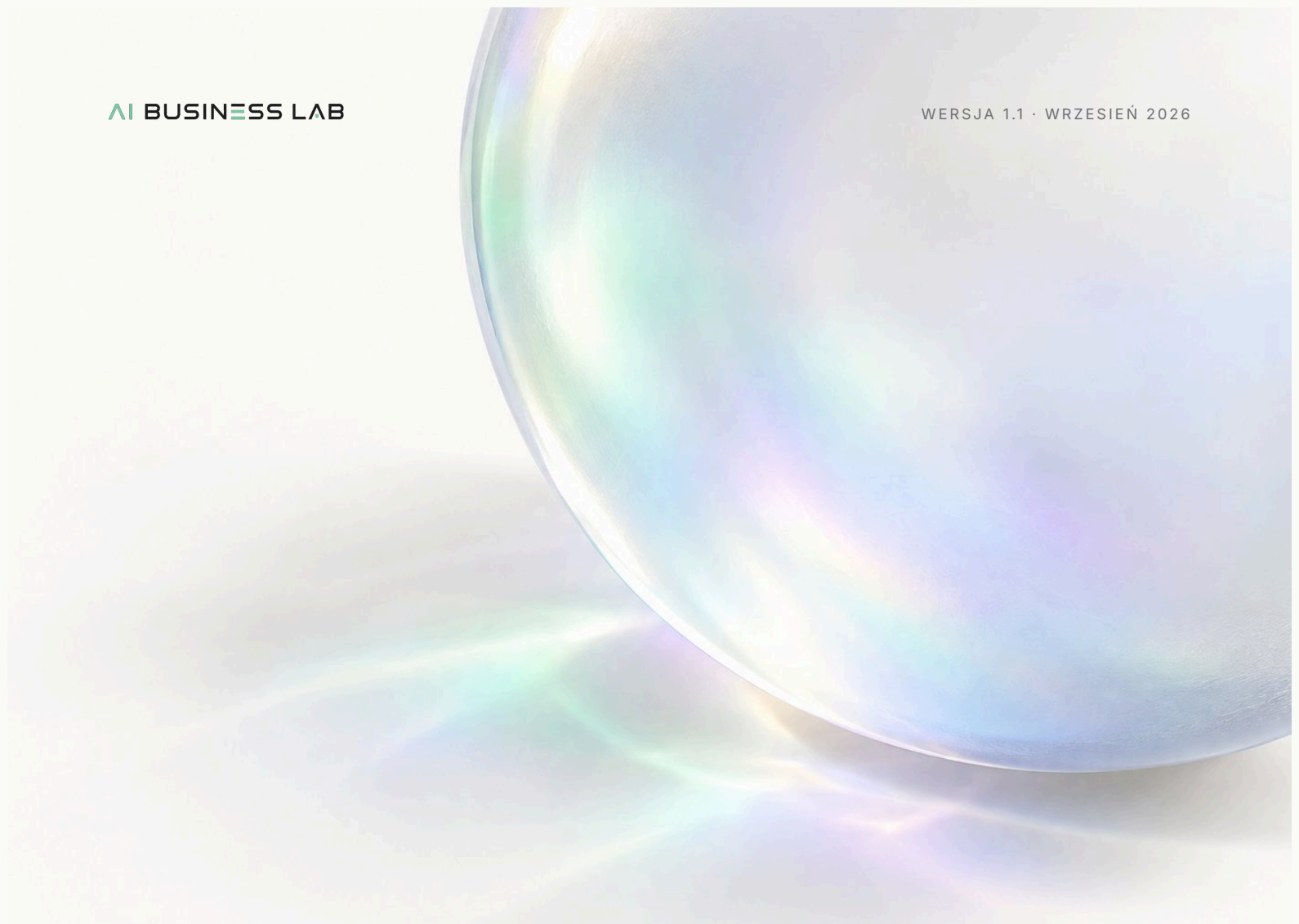

STEROWNIA · BEZPIECZEŃSTWO DANYCH

Bezpieczeństwo i zgodność

Jak chronimy dane klientów: gdzie są przechowywane, kto ma do nich dostęp, jak wykonujemy kopie zapasowe, z jakich dostawców korzystamy i co robimy w razie incydentu lub awarii.

DOSTAWCA

CLEARWISE sp. z o.o.

marka AI Business Lab · NIP 5833541389 · KRS 0001181410

KONTAKT W SPRAWACH BEZPIECZEŃSTWA

kontakt@aibusinesslab.pl

umowy, DPA i RODO: legal@aibusinesslab.pl

W skrócie

AI Business Lab wdraża automatyzacje AI i prowadzi Sterownię, panel, w którym firmy zarządzają treściami, leadami i kampaniami. Dane klientów trzymamy w bazie w Unii Europejskiej, każdy dostęp jest uwierzytelniony, a wrażliwe dane dostępowe szyfrujemy. Poniżej opisujemy konkretne mechanizmy, nie ogólne deklaracje.

- **Baza danych w UE**
  Dane Sterowni w Supabase, region Frankfurt (eu-central-1).
- **Szyfrowanie**
  TLS z HSTS dla całego ruchu, AES-256-GCM dla haseł i kluczy do narzędzi klientów.
- **Kontrola dostępu**
  Row Level Security na wszystkich tabelach, role w zespole, blokada po 5 błędnych logowaniach.
- **Codzienne kopie**
  Automatyczna kopia bazy każdej doby, przechowywana 7 dni.
- **Zero danych kart**
  Płatności obsługuje PayU (PCI DSS). Pełny numer karty nigdy nie trafia do naszych systemów.
- **RODO i DPA**
  Umowa powierzenia przetwarzania danych na wniosek klienta, lista podprocesorów jawna.

01 RODO i umowa powierzenia (DPA)

Dla danych, które klient wprowadza do Sterowni lub które przetwarzamy przy wdrożeniu, działamy jako podmiot przetwarzający w rozumieniu art. 28 RODO. Dla własnych danych kontaktowych i rozliczeniowych jesteśmy administratorem.

- Umowę powierzenia przetwarzania danych (DPA) zawieramy na wniosek klienta. Wystarczy napisać na legal@aibusinesslab.pl.
- Przetwarzamy dane wyłącznie w celu wykonania umowy i na udokumentowane polecenie klienta. Nie sprzedajemy danych i nie wykorzystujemy ich do własnego marketingu.
- Przekazanie danych poza EOG odbywa się wyłącznie na podstawie decyzji o adekwatności (EU-US Data Privacy Framework) albo standardowych klauzul umownych Komisji Europejskiej.
- Pomagamy klientowi realizować prawa osób, których dane dotyczą: dostęp, sprostowanie, usunięcie, przeniesienie danych.
- Po zakończeniu umowy usuwamy lub zwracamy dane klienta, z wyjątkiem danych, które musimy przechowywać z mocy prawa (np. faktury).

02 Gdzie i jak przechowujemy dane

Dane klientów trafiają do jednej produkcyjnej bazy danych w Unii Europejskiej. Aplikacja i procesy działają u wyspecjalizowanych dostawców infrastruktury.

- Cały ruch do strony i do Sterowni jest szyfrowany (HTTPS/TLS). Sterownia wymusza HTTPS nagłówkiem HSTS na 2 lata.
- Hasła i klucze API, które klient podpina do swoich narzędzi (np. WordPress, konta reklamowe, mailing), są szyfrowane algorytmem AES-256-GCM z osobnym kluczem dla każdego rodzaju danych.
- Hasła użytkowników Sterowni przechowujemy wyłącznie jako skrót bcrypt, nigdy jawnym tekstem.
- Dane kart płatniczych obsługuje PayU S.A. (PCI DSS). Otrzymujemy tylko potwierdzenie płatności i token karty.

Komponent	Dostawca	Lokalizacja
Baza danych i pliki Sterowni	Supabase (PostgreSQL 17, plan Pro)	UE, Frankfurt
Aplikacja Sterowni (warstwa serwerowa)	Vercel (plan Pro)	USA
Procesy w tle i automatyzacje	Hetzner (serwer dedykowany)	UE, Niemcy
Strona aibusinesslab.pl	lh.pl	Polska

Komponent	Dostawca	Lokalizacja
Poczta firmowa	Google Workspace	UE / USA

03 Dostępy i zasada najmniejszych uprawnień

- Row Level Security jest włączone na wszystkich tabelach bazy. Tabele bez jawnej polityki dostępu są zamknięte dla każdego poza serwerem aplikacji.
- Klucz serwisowy bazy danych jest używany wyłącznie po stronie serwera i nigdy nie trafia do przeglądarki.
- Role w zespole klienta: właściciel, administrator, pracownik. Klucze API do narzędzi widzi tylko właściciel konta.
- Po 5 nieudanych próbach logowania konto jest blokowane na 15 minut. Dodatkowo obowiązuje limit prób z jednego adresu IP.
- Hasło do Sterowni ma co najmniej 8 znaków, małą i wielką literę oraz cyfrę lub znak specjalny.
- Sesja to losowy token w ciasteczku httpOnly i secure, niedostępnym dla skryptów na stronie. Czas logowania nie zdradza, czy dane konto istnieje.
- Serwer infrastruktury: logowanie administratora wyłącznie kluczem SSH, firewall domyślnie blokujący ruch przychodzący i automatyczne banowanie adresów, które próbują zgadywać hasła (fail2ban).
- Kod źródłowy jest w prywatnych repozytoriach, a wdrożenia przechodzą przez zautomatyzowany proces budowania.

04 Kopie zapasowe, logi i monitoring

- Automatyczna, pełna kopia bazy danych wykonywana codziennie i przechowywana przez 7 dni u Supabase, w tej samej lokalizacji co baza.
- Na żądanie klienta odtwarzamy jego dane z wybranej kopii z ostatnich 7 dni.
- Na żądanie klienta, także po zakończeniu współpracy, przekazujemy pełny eksport jego danych w otwartym formacie (CSV lub JSON).
- Każda próba logowania jest zapisywana w trwałym dzienniku: czas, adres IP, przeglądarka i wynik.
- Zmiany rozliczeń oraz dodanie lub usunięcie kluczy dostępowych klienta są rejestrowane w osobnym dzienniku zmian.
- Agent nadzoru sprawdza procesy na serwerze, automatycznie restartuje te, które przestały działać, i wysyła alert do zespołu.
- Codzienny przegląd alarmów aplikacji trafia bezpośrednio do administratora.

05 Dostawcy AI i przetwarzanie przez modele

Modele AI generują teksty, grafiki i transkrypcje na podstawie briefu firmy klienta. Korzystamy z nich wyłącznie przez interfejsy API dla firm, a nie przez aplikacje konsumenckie. Od września

2026 AI Business Lab jest OpenAI Select Partner w programie OpenAI Partner Network.

- Nie wykorzystujemy danych klientów do trenowania modeli AI. OpenAI, nasz główny dostawca modeli, zgodnie z warunkami swojego API nie trenuje modeli na przesyłanych danych.
- Do modeli trafia tylko to, co jest potrzebne do wykonania zadania: brief, materiały marki i treść polecenia. Nie przekazujemy im haseł, kluczy dostępowych ani danych kart.
- Ruch do modeli językowych przechodzi przez Vercel AI Gateway, co daje jedno kontrolowane miejsce wyjścia danych i możliwość szybkiej zmiany dostawcy.
- Klient może podpiąć własny klucz OpenAI (BYOK). Wtedy zapytania idą na jego konto i na jego warunkach umownych.
- Każdą treść wygenerowaną przez AI klient może zaakceptować, poprawić albo odrzucić przed publikacją. AI nie podejmuje wobec nikogo decyzji wywołujących skutki prawne.

06 Procedura na wypadek incydentu

- Wykrycie: alerty z monitoringu, dziennik logowań i zgłoszenia na kontakt@aibusinesslab.pl.
- Ograniczenie skutków: blokada kont, unieważnienie sesji, wymiana kluczy i haseł, odcięcie zagrożonej integracji.
- Ocena: ustalamy, jakich danych i których klientów dotyczy zdarzenie oraz jakie niesie ryzyko.
- Powiadomienie: klienta, którego dane dotyczy incydent, informujemy bez zbędnej zwłoki, wraz z opisem zdarzenia, zakresu danych i podjętych działań (art. 33 ust. 2 RODO).
- Gdy jesteśmy administratorem danych, zgłaszamy naruszenie do Prezesa UODO w ciągu 72 godzin od jego stwierdzenia, jeśli wymaga tego art. 33 RODO.
- Wnioski: po zamknięciu incydentu dokumentujemy przyczynę i wdrażamy poprawki, żeby zdarzenie się nie powtórzyło.

07 Zgłaszanie awarii i ciągłość działania

Awaria to coś innego niż incydent bezpieczeństwa: system nie działa albo działa źle, choć dane są bezpieczne. Dla obu sytuacji klient ma jasną ścieżkę i wie, co się dzieje.

- Zgłoszenie: e-mailem na kontakt@aibusinesslab.pl albo bezpośrednio do opiekuna wdrożenia. Potwierdzamy je i przypisujemy osobę odpowiedzialną.
- Priorytet: awaria, która zatrzymuje pracę zespołu klienta (np. brak logowania), ma pierwszeństwo przed wszystkimi innymi pracami. Czasy reakcji zapisujemy w umowie z klientem.
- Informacja o postępie: klient dostaje wiadomość o przyczynie, podjętych działaniach i przewidywanym czasie naprawy, aż do zamknięcia zgłoszenia.
- Po naprawie: opisujemy, co się stało i co zmieniliśmy, żeby awaria się nie powtórzyła.
- Ciągłość działania: dla każdego wdrożenia prowadzimy aktualną dokumentację. Dane i konfigurację klienta możemy w każdej chwili przekazać w pełnym eksporcie, a utrzymanie systemu przekazać innej firmie wskazanej przez klienta.
- Przy wdrożeniach dedykowanych umowa może dodatkowo przewidywać przekazanie kodu rozwiązania albo jego depozyt na wypadek zakończenia współpracy.

08 Lista podprocesorów

Dostawcy, którzy mogą przetwarzać dane klientów w związku ze świadczeniem usług. Zakres zależy od funkcji, z których korzysta klient.

Podprocesor	Cel	Lokalizacja
Supabase Inc.	Baza danych i pliki Sterowni	UE (Frankfurt)
Vercel Inc.	Hosting aplikacji, AI Gateway (pośrednik do modeli AI)	USA
Hetzner Online GmbH	Serwer procesów w tle i automatyzacji	UE (Niemcy)
LH.pl sp. z o.o.	Hosting strony aibusinesslab.pl	Polska
OpenAI	Generowanie tekstów i grafik, transkrypcja	USA
Inni dostawcy modeli językowych dostępni przez Vercel AI Gateway	Generowanie tekstów	USA / inne
Groq Inc.	Transkrypcja wiadomości głosowych	USA
Higgsfield	Generowanie grafik i wideo	USA
PayU S.A.	Płatności online i cykliczne	Polska
Resend Inc.	Wysyłka wiadomości systemowych i faktur	USA
Meta Platforms Ireland	Publikacja treści i kampanie z kont klienta	UE / USA
Zernio	Publikacja postów w mediach społecznościowych	UE (Hiszpania) / inne
Nango Inc.	Bezpieczne łączenie kont klienta (OAuth)	USA
Apify, Firecrawl, Tavily, Exa	Wyszukiwanie publicznych informacji rynkowych	USA
Google (Workspace, Analytics, Calendar)	Poczta, analityka, rezerwacje	UE / USA
Telegram, Slack	Powiadomienia, tylko gdy klient je włączy	UE / USA

Kontakt

Na prośbę działu bezpieczeństwa lub działu prawnego odpowiadamy na kwestionariusze bezpieczeństwa i przygotowujemy umowę powierzenia przetwarzania danych.

BEZPIECZEŃSTWO I INCYDENTY
kontakt@aibusinesslab.pl

UMOWY, DPA, RODO
legal@aibusinesslab.pl

SPÓŁKA
CLEARWISE sp. z o.o., ul. Zawodzie 20, 80-726 Gdańsk

REJESTR
NIP 5833541389 · KRS 0001181410

Dokument opisuje stan systemów na dzień publikacji wersji. Aktualna wersja: aibusinesslab.pl/bezpieczenstwo. Szczegóły przetwarzania danych osobowych: aibusinesslab.pl/polityka-prywatnosci.