AKTUALIZACJA V2 POPRAWIONA

Wrzucasz poufne umowy i faktury do Claude'a?

Zobacz, co NAPRAWDĘ dzieje się z Twoimi danymi (i jak robić to bezpiecznie).



GROWTH AI

Piotr Cieluchowski in @cieluchowski

Masz płatny plan. Myślisz,
że jesteś w 100% bezpieczny?

Masz płatny plan. Myślisz, że jesteś w 100% bezpieczny?



Wielu przedsiębiorców wrzuca do czatu (Claude.ai / Claude for Work) pliki z danymi osobowymi, umowami NDA czy finansami. W końcu płacą za wersję Pro lub Max.

Mam dobrą i złą wiadomość.

✅ Dobra wiadomość: API = zero treningu.

Claude API i **Claude Enterprise**: Twoje dane NIE są wykorzystywane do trenowania modeli — gwarancja w umowie.

Claude.ai (Free / Pro / Max): od sierpnia 2025 dane **MOGĄ** być używane do treningu — chyba że zrobisz opt-out w ustawieniach prywatności.

sprawdź ustawienia!

✗ Zła wiadomość: Claude.ai to produkt konsumencki.

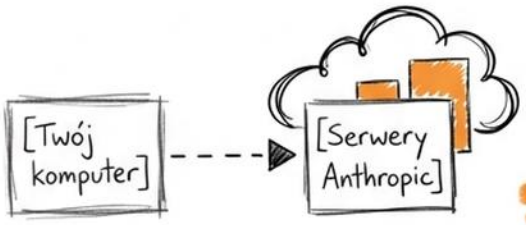
W świetle RODO Claude.ai to produkt dla konsumentów.

Anthropic **NIE podpisuje DPA** (Data Processing Agreement, art. 28 RODO) dla użytkowników Claude.ai — tylko dla klientów Enterprise.
Bez DPA brak formalnej podstawy powierzenia danych osobowych klientów.

brak DPA = ryzyko RODO



Zrozum ryzyko: Przetwarzanie w chmurze ☁️



Zrozum ryzyko: Przetwarzanie w chmurze ☁️

Kiedy wgrywasz fakturę do czatu i prosisz o podsumowanie, plik opuszcza Twoją firmę i trafia na serwery Anthropic. Choć technicznie bezpieczne, łamie to wewnętrzne procedury bezpieczeństwa (DLP) w wielu korporacjach.

Rozwiązanie nr 1: Claude Enterprise + DPA + ZDR 📄

Claude.ai (Chat)	Claude Enterprise (API) ✅
❌ →	Jeśli przetwarzasz dane osobowe, medyczne lub finansowe — potrzebujesz **Claude Enterprise** z podpisanym **DPA (Data Processing Agreement, art. 28 RODO**) i włączonym **ZDR (Zero Data Retention)**. DPA = formalna podstawa powierzenia. ZDR = dane nie są zapisywane na serwerach Anthropic.

DPA = art. 28 RODO

ZDR = zero retencji



→

Złota zasada: Co możesz wrzucać, czego nie ⚖️



Rozwiązanie nr 2: Lokalne modele AI 💻



Dane zostają na laptopie

Dla najwrażliwszych danych: modele AI na Twoim komputerze lub serwerze firmowym. Dane zostają u Ciebie — zero cloud.

zero danych publicznych

Opcje: **LM Studio** z Llama 4, **Ollama** z Mistral, prywatny Claude na **AWS Bedrock** albo **Google Vertex AI** (VPC).

5 zasad bezpiecznego AI w Twojej firmie

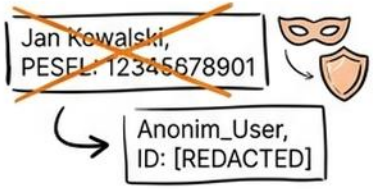
1. Określ kategorie danych wrażliwych w firmie



2. Używaj Claude Enterprise + DPA + ZDR dla danych osobowych

Rekomendacja dla EU/RODO:

3. Anonimizuj dane przed wklejeniem do czatu



4. Rozważ lokalne modele dla najbardziej poufnych akt



```
local_model_run(confidential_data)
```

5. Napisz wewnętrzną politykę AI dla pracowników



POPRAWIONA V2

Chcesz wiedzieć więcej o bezpiecznym AI dla biznesu?



👉 Obserwuj, żeby nie przegapić kolejnych części.

💡 Zapisz ten post — przyda się przy następnym audycie danych.

💬 Napisz w komentarzu: jak Ty chronisz dane firmowe w AI?

Przewodnik dla biznesu — 1/3 · V2

GROWTH AI