AKTUALIZACJA V2 POPRAWIONA

Twoja firma nie ma polityki AI? To większy problem niż myślisz. ⚠

Krok po kroku: jak napisać politykę AI, która naprawdę chroni Twoją firmę.



GROWTH AI

Piotr Cieluchowski in @cieluchowski

RECAP

W poprzedniej części: ryzyka, które już znasz 🔒

Jeśli trafiłeś tutaj po raz pierwszy — w części 1 wyjaśniłem:

- Dlaczego Claude.ai (Chat) nie ma DPA z firmą
- Co się dzieje z Twoimi danymi na serwerach Anthropic
- Kiedy warto Claude Enterprise + DPA + ZDR, a kiedy lokalne modele

Ta część idzie krok dalej: jak to urządzić formalnie w firmie?

Obejrzyj cz. 1 (V2) w poprzednim poście





Co to jest polityka AI i po co Ci ona? 📄

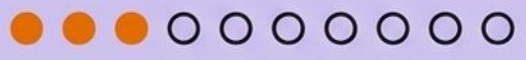
Co to jest polityka AI i po co Ci ona? 📄

Polityka AI to wewnętrzny dokument firmy, który określa:

- Kto może używać AI i do jakich zadań
- Jakich danych **NIE** wolno wrzucać do czatu
- Jakie narzędzia AI są zatwierdzone
- Co robić w razie incydentu + logowanie użycia AI
- Datę przeglądu (co 6 miesięcy — AI zmienia się szybko)

Bez niej pracownicy robią co chcą. Z nią — wiesz co się dzieje.







Krok 1: Inwentaryzacja — czego AI już używacie? 🔍

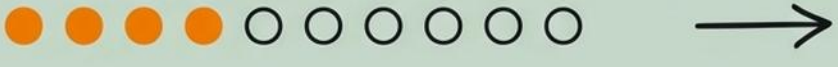
1 Krok 1: Inwentaryzacja — czego AI już używacie? 🔍

Zanim napiszesz politykę, sprawdz co jest w firmie. Zapytaj każdego działu:

- Z jakich narzędzi AI korzystacie? (ChatGPT, Claude, Copilot...)
- Do jakich zadań ich używacie?
- Jakie dane w nie wchodzić?



Efekt: lista narzędzi do zatwierdzenia lub zablokowania.



Krok 2: Klasyfikacja danych — co wolno, czego nie 🏷️

bezpieczna strefa

	Przykłady	Działanie
ZIELONE	ogólne pytania, research, szablony bez danych osobowych.	✅ Możesz wrzucać do dowolnego AI (Claude.ai, ChatGPT, Gemini, Mistral Le Chat).
ŻÓŁTE	wewnętrzne dokumenty firmowe, dane klientów zanonimizowane.	⚠️ Tylko Claude Enterprise + DPA, Microsoft Copilot lub Mistral EU — nie Chat.
CZERWONE	umowy NDA, faktury z NIP, dane PESEL, dokumentacja medyczna.	❌ Zakaz. Tylko lokalne modele AI lub Claude Enterprise + DPA + ZDR.



Krok 3: Lista zatwierdzonych narzędzi AI ✅

Zgodne z regulacjami RODO i polityką bezpieczeństwa!

ZATWIERDZONE (podpisane DPA + weryfikacja):

- Claude Enterprise + DPA + ZDR (dane osobowe) ✅
- Microsoft Copilot (tenant Microsoft 365) ✅
- Mistral Le Chat / Aleph Alpha (serwery w UE) ✅
- Lokalne modele na własnych serwerach ✅

NIE ZATWIERDZONE (brak DPA lub brak weryfikacji):

- Claude.ai Chat (brak DPA) ❌
- Bezpłatne wersje ChatGPT, Gemini ❌
- Dowolne narzędzie bez audytu bezpieczeństwa ❌

RYZYKO! Brak ochrony danych osobowych i własności intelektualnej.





Krok 4: Szkolenie zespołu — 10 minut, które zmienia wszystko 🎯

Pracownicy nie łamią zasad z złej woli — po prostu nie wiedzą.

Minimum szkoleniowe **(10-15 min,** może być wideo lub PDF):

- Co wolno, czego nie wolno wrzucać do AI
- Jak rozpoznać dane wrażliwe
- Co robić gdy przypadkowo wrzuciłem złe dane

Kluczowe tematy

Dodaj quiz na końcu. Udokumentuj kto przeszedł.

Sprawdź wiedzę

Krok 5: Procedura incydentowa — co gdy coś poszło nie tak? 🚨

Jeśli pracownik wrzucił wrażliwe dane do AI:

1. Natychmiast poinformuj przełożonego oraz DPO (lub osobę odpowiedzialną za ochronę danych)
2. Udokumentuj: co, kiedy, jakie narzędzie, jakie dane
3. Skontaktuj się z dostawcą AI (Anthropic/OpenAI/Mistral)
4. Ocena ryzyka: czy niezbędne zgłoszenie do UODO? (72h!)
5. Aktualizacja procedur i szkolenie zespołu po incydencie



Gotowy szablon polityki AI — pobierz i dostosuj 📥

Nie zaczynaj od zera. Dobry szablon zawiera:

- Definicje i zakres (kogo dotyczy polityka)
- Klasyfikację danych (zielone / żółte / czerwone)
- Listę zatwierdzonych i zakazanych narzędzi + DPA
- Logowanie użycia AI + audyt co 6 miesięcy
- DPIA (art. 35 RODO) dla systemow przetwarzających dane osobowe
- Procedurę szkoleniową i incydentową
- Datę przeglądu (polityka starzeje się szybko!)

DPIA = ocena skutków

Szablon: link w pierwszym komentarzu pod postem.

POPRAWIONA V2

To była część 2/3. W części 3: AI w kontraktach i NDA 💼



👉 Obserwuj, żeby nie przegapić części 3.

💾 Zapisz ten post — szablon polityki AI czeka w komentarzach.

💬 Napisz: czy Twoja firma ma już politykę AI?

Zapowiedź cz. 3: Jak ocenić ryzyko AI w umowach z klientami i co warto dodać do klauzul NDA w 2026 roku.