KD-2

Robi Się Samo
stan na XI 2026

Co wolno wkleić do AI – światło drogowe danych

Najpierw jedno pytanie: z jakiego konta korzystasz?

- **Konto firmowe** – narzędzie od firmy, która ma umowę z jego dostawcą.
- **Konto prywatne** (także płatne) – Twój własny ChatGPT, Gemini, Claude albo Copilot. Twoja firma nie ma umowy z jego dostawcą.
- **Korzystasz bez logowania?** Traktuj to jak konto prywatne.
- **Masz własną firmę?** Ty decydujesz i Ty odpowiadasz. Dane klientów wklejasz tylko na koncie firmowym z umową powierzenia danych (DPA). W niej dostawca zobowiązuje się chronić dane, które mu dajesz. „Zgoda na piśmie" to u Ciebie ta umowa i Twoja umowa z klientem.
- **Nie wiesz, które konto masz?** Zapytaj dział IT albo przełożonego. To zwykłe pytanie.

ZIELONE	ŻÓŁTE	CZERWONE	NIGDY
wolno wszędzie	tylko w narzędziu firmowym	tylko gdy firma na piśmie pozwala w tym narzędziu	nigdzie

● **ZIELONE – wolno wszędzie, na każdym koncie:** to, co już jest publiczne (strona firmy, przepisy, artykuły) · ogólne pytania · Twój tekst bez nazwisk, nazw klientów i liczb firmy · zmyślone przykłady.

▲ **ŻÓŁTE – tylko na koncie firmowym:** procedury, szablony, notatki ze spotkań, szkice maili i raportów. Zanim wkleisz, usuń nazwiska, telefony, adresy i liczby, których AI nie potrzebuje.

■ **CZERWONE – tylko gdy firma na piśmie pozwala w tym narzędziu:**

- dane o ludziach: nazwiska, PESEL, wynagrodzenia, oceny, zdrowie, zdjęcia, nagrania
- dokumenty i dane klientów, wszystko objęte umową o poufności
- finanse, marże, plany i oferty, które nie są publiczne
- kod programów firmy i opisy zabezpieczeń

✗ **NIGDY, NIGDZIE:** hasła, kody dostępu, numery kart płatniczych, skany dowodów osobistych.

Gdy pasuje kilka kolorów, wygrywa najsurowszy.

Trzy nawyki

1. Masz wątpliwość? Nie wklejaj – zapytaj.
2. „Klient A" zamiast nazwiska to dobry nawyk, ale nie przepustka do prywatnego czatu. Jeśli da się odgadnąć, kto to, dane nadal są osobowe.
3. Przy sprawach z pracy nie oceniaj odpowiedzi kciukiem. U części dostawców, także w aplikacji Claude na koncie firmowym, kliknięcie wysyła całą rozmowę i pozwala użyć jej do treningu.

Coś czerwonego trafiło do czatu? Nie ukrywaj. Usuń rozmowę i od razu powiedz: ☐ IT ☐ osobie od ochrony danych ☐ przełożonemu – _____. Przy danych osobowych firma

może musieć zgłosić to do Urzędu Ochrony Danych Osobowych. Ma na to najwyżej 72 godziny od chwili, gdy się o tym dowie. Liczy się szybkość, nie wstyd.

⚠ **UWAGA**

Ostrzega sam producent

Google pisze o Gemini na koncie prywatnym: „Nie podawaj informacji poufnych, których nie chcesz udostępniać weryfikatorom (...)". Dlatego tam wklejasz tylko dane zielone.

Ta karta nie zastępuje zasad AI Twojej firmy. Jeśli firma je ma, są ważniejsze.

Wszystko, co musisz wiedzieć o AI · Kompendium Robi Się Samo · Stan na XI 2026
Źródła: UODO, listy pytań RODO i AI (2026) · RODO art. 28 i 33 · dokumentacja Google, OpenAI, Anthropic, Microsoft (XI 2026) · wpisy KD.3–KD.8 w „Skąd to wiemy"
Możesz wydrukować i przekazać bez zmian · CC BY-NC-ND 4.0 · **robisiesamo.pl/kompendium**

robisiesamo.pl/kompendium