



Twój zespół korzysta z AI. Dane klientów zostają u Ciebie.

Do Not Feed AI podmienia dane osobowe i poufne na realistyczne dane fikcyjne - lokalnie, w przeglądarce i na Twoim komputerze - zanim trafią do ChatGPT, Claude, Gemini czy Copilota. Oryginały wracają w odpowiedzi modelu. Nic nie opuszcza urządzenia, nie ma żadnego serwera pośredniczącego.

- zero połączeń sieciowych
- działa w Chrome, Edge i Brave
- ChatGPT · Claude · Gemini · Copilot



DLACZEGO TO JEST POTRZEBNE

Publiczny czat AI to kanał, którym dane wychodzą z firmy.

Pracownicy każdego dnia wklejają do ChatGPT czy Copilota dane klientów (nazwiska, PESEL, adresy, treść umów), zawartość arkuszy i dokumentów, a zespoły techniczne - konfiguracje z hasłami i adresami serwerów. Każde takie wklejenie to przekazanie danych poza organizację, zwykle poza EOG, bez kontroli nad dalszym przetwarzaniem. Zakaz korzystania z AI nie działa: ludzie korzystają i tak, tylko poza wiedzą działu IT. Do Not Feed AI usuwa ryzyko u źródła, nie zabierając zespołowi narzędzia.

CO WYKRYWA

Reguły i sumy kontrolne dopasowane do polskich danych.

Imię i nazwisko

słownik 1352 imion, także w przypadkach zależnych

PESEL

suma kontrolna albo wiarygodna data urodzenia

NIP, REGON, IBAN, nr dowodu

z walidacją, więc numer zamówienia nie jest NIP-em

Telefon i e-mail

krajowe i zagraniczne; e-mail we wzorcu osoby

Adres, kod i miasto

„ul. Długa 7” i „Skośna 8” obok innych danych

Nazwa firmy

Sp. z o.o., S.A., Sp. j., Ltd., GmbH

Własne frazy

nazwy projektów, klientów, produktów

Kolumny w arkuszach

nagłówek ustala typ całej kolumny



PRZEPŁYW DANYCH

Granica komputera, której oryginały nie przekraczają.

Maskowanie dzieje się na Twoim urządzeniu - w przeglądarce dla tekstu, w companionie dla plików. Do usługi AI trafiają wyłącznie dane fikcyjne, a mapa powiązań i oryginały nigdy nie opuszczają komputera. Odpowiedź modelu jest przywracana lokalnie, więc na ekranie widzisz prawdziwe wartości.



01 · PRZED WYSŁANIEM

Przechwycenie

Wtyczka zatrzymuje wysyłkę w polu czatu i wykrywa dane wrażliwe, zanim wiadomość opuści przeglądarkę.

02 · ZAMIANA

Dane fikcyjne

Zamiast prawdziwych wartości model dostaje realistyczne zamienniki z poprawnymi sumami kontrolnymi. Nie „poprawia” danych i odpowiada tak samo dobrze.

03 · WYSYŁKA

Do modelu idą zamienniki

Mapa powiązań oryginał-zamiennik zostaje wyłącznie na urządzeniu, zaszyfrowana. Do dostawcy AI nie trafia żadna prawdziwa dana.

04 · ODPOWIEDŹ

Oryginały wracają

W odpowiedzi modelu zamienniki są w locie podmieniane z powrotem na prawdziwe wartości - także w odmienionej formie i w plikach.



KONKRETNE MECHANIZMY, NIE OBIETNICE

Dane nie opuszczają urządzenia. To można sprawdzić.

Zero sieci

Wtyczka ma tylko dwa uprawnienia: pamięć lokalna i połączenie z companionem. Companion nie zawiera żadnej biblioteki sieciowej. Brak telemetrii i licencji online.

Sesja wygasa

Po 1, 7 lub 30 dniach albo nigdy - do wyboru. Po wygaśnięciu klucz znika razem z mapą, dawnych rozmów nie da się już odtworzyć.

Praca offline

Całość działa bez połączenia z internetem po stronie narzędzia. Nie ma serwera producenta, który mógłby zobaczyć dane albo paść ofiarą wycieku.

Mapa zamienników zaszyfrowana

AES-256-GCM w pamięci przeglądarki, klucz w pęku kluczy systemu (Keychain, Credential Manager / DPAPI). Bez companiona mapa żyje tylko w pamięci.

Pliki nigdy na dysku

Plik z czatu jest maskowany w pamięci i od razu odsyłany. Companion nie zostawia kopii roboczej, awaria nie zostawia oryginału.

Kod do audytu

Companion to jedna binarka w języku Rust, bez zależności sieciowych; reguły i algorytm są jawne i możliwe do przejrzania przez dział bezpieczeństwa.

RODO I NIS 2

Przepisy nie mówią „nie używaj AI”. Mówią „pseudonimizuj i szyfruj”.

RODO
art. 4 pkt 5

Definicja pseudonimizacji: dane przetworzone tak, by bez „dodatkowych informacji” nie dało się ich przypisać osobie, a te informacje przechowywane osobno. **W narzędziu:** do czatu trafiają dane fikcyjne, a mapa powiązań leży osobno, zaszyfrowana, na urządzeniu użytkownika.

RODO
art. 5 ust. 1

Minimalizacja oraz integralność i poufność danych. **W narzędziu:** dostawca modelu nie potrzebuje prawdziwego PESEL-u ani nazwiska, żeby napisać pismo - dostaje tylko to, co niezbędne, a maskowanie działa automatycznie, także w plikach.

RODO
art. 25 i 32

Ochrona danych w fazie projektowania oraz pseudonimizacja i szyfrowanie jako środki bezpieczeństwa. **W narzędziu:** jedno i drugie wbudowane w sposób przetwarzania, nie w regulamin; wdrożone raz, polityką, działają przy każdym użyciu.

NIS 2
art. 21

Proporcjonalne środki techniczne zarządzania ryzykiem: bezpieczeństwo łańcucha dostaw, cyberhigiena, polityki kryptografii. **W narzędziu:** dostawca AI to usługodawca w łańcuchu dostaw; profil techniczny zatrzymuje hasła, klucze i adresy infrastruktury przed wystaniem.

Do Not Feed AI jest środkiem technicznym wspierającym zgodność, a nie zgodnością samą w sobie. Ocenę adekwatności środków podejmuje administrator danych. Podstawa: rozporządzenie (UE) 2016/679 (RODO) i dyrektywa (UE) 2022/2555 (NIS 2).



DLA DZIAŁÓW IT, DEVOPS I ADMINISTRATORÓW **PRO**

Konfiguracje, logi i skrypty bez sekretów i nazw infrastruktury.

Profil techniczny maskuje hasła, tokeny i klucze (ponad 220 formatów dostawców: AWS, GitHub, GitLab, Slack, Stripe, OpenAI, klucze prywatne PEM, hasła w connection stringach), adresy hostów, adresy IP i loginy. Struktura zostaje, więc model dalej rozumie plik: `db-prod-01.eu.acme.internał` staje się `db-prod-01.eu.zorin.internał`, klucz `AKIA...` nadal wygląda jak klucz AWS, a poprawiony plik wraca z prawdziwymi wartościami. Reguły techniczne działają wyłącznie w companionie, nie w kodzie wtyczki.

LICENCJE - OFFLINE, BEZ SERWERA

Trzy poziomy. Jeden podpisany plik na całą organizację.

Free

JEDNA OSOBA · BEZPŁATNIE

Maskowanie danych osobowych w tekście czatu, podgląd przed wysłaniem i automatyczne przywracanie odpowiedzi.

Bez limitu czasu.

Pro

NA STANOWISKO

Wszystko z Free oraz pliki, dane techniczne (sekrety, hosty, IP), własne frazy, tryb ręczny i sesja szyfrowana na dysku.

7 dni pełnego Pro po instalacji, bez podawania danych.

Business

NA FIRMĘ

Wszystko z Pro oraz wspólny słownik firmowy i wdrożenie licencji przez MDM lub politykę - jeden plik dla wszystkich stanowisk.

Rozliczenie i liczba stanowisk po stronie umowy.

Licencja to czytelny plik podpisany kryptograficznie (Ed25519), jeden na firmę, ten sam na wszystkich stanowiskach - egzekwowane są data ważności i poziom, nie liczba stanowisk. Brak serwera licencyjnego i połączeń z zewnątrz; po wygaśnięciu 14 dni okresu przejściowego, potem poziom Free.

Wdrażasz raz. Chroni każdego pracownika, na każdym czacie.

Wtyczka trafia na wszystkie stanowiska jedną polityką przeglądarki, companion instaluje się bez uprawnień administratora, licencja to jeden plik. Bez serwera, bez kont, bez szkoleń.

STRONA

donotfeedai.com

KONTAKT

kontakt@donotfeedai.pl

DOSTAWCA

Sebastian Obara It&Consulting



INSTALACJA W CZTERY KROKI • MACOS

Masz dwa pliki. Kwadrans i gotowe.

COMPANION (PLIKI)

donotfeedai-X.Y.Z.pkg

Instalator macOS, podpisany i notaryzowany.

WTYCZKA (PRZEGLĄDARKA)

donotfeedai-wtyczka-chrome-X.Y.Z.zip

Chrome, Edge, Brave, Chromium.

1

Zainstaluj companion

Dwuklik na **donotfeedai-X.Y.Z.pkg** i podaj hasło administratora. Instalator sam rejestruje połączenie z przeglądarką. Jest podpisany i notaryzowany, więc Gatekeeper nie blokuje uruchomienia.

2

Załaduj wtyczkę

Rozpakuj **donotfeedai-wtyczka-chrome-X.Y.Z.zip**. Wejdź w **chrome://extensions** (Edge: **edge://extensions**), włącz **Tryb dewelopera**, kliknij **Załaduj rozpakowane** i wskaż rozpakowany folder (ten z plikiem **manifest.json**). Nie przenoś potem tego folderu.

3

Zrestartuj przeglądarkę

Zamknij ją całkowicie (Cmd+Q, samo zamknięcie okna nie wystarczy) i otwórz ponownie. Połączenie z companionem jest odczytywane przy starcie.

4

Sprawdź i wczytaj licencję

Kliknij ikonę wtyczki - z prawej otworzy się panel ze statusem **Companion: połączony**. Firmową licencję wczytasz w panelu: **Wczytaj plik licencji** i wskaż plik **.lic**. Bez licencji masz 7 dni pełnego Pro.

Wdrożenie masowe: w organizacji companion i plik licencji rozkłada MDM albo polityka przeglądarki, a wtyczkę wymusza polityka instalacji - użytkownik nie robi nic z powyższych kroków. **Docelowo** wtyczka będzie w Chrome Web Store: instalacja jednym kliknięciem, bez trybu dewelopera i bez restartu. Windows i Firefox: patrz osobna instrukcja instalacji.