



JAK PRACUJEMY

Jak chronimy dane Państwa firmy

W wielu firmach największe ryzyko pojawia się jeszcze przed wdrożeniem: pracownicy wklejają firmowe dane do prywatnych, darmowych chatów AI, bo nikt nie dał im lepszego narzędzia. **Nasze wdrożenie porządkuje ten obszar.** Poniżej zasady, których trzymamy się w każdym projekcie.

Dziewięć zasad

1. Tylko firmowe wersje AI

Korzystamy z płatnych usług z umową. Państwa dane nie służą do trenowania modeli AI.

2. Dostęp tylko do tego, co potrzebne

System widzi wyłącznie dane potrzebne do swojego zadania. Tam, gdzie wystarczy odczyt, nie ma prawa zapisu.

3. Człowiek zatwierdza

Mail do klienta, zapis w systemie firmowym, każda nieodwracalna akcja: zatwierdza ją wskazana osoba, nie AI.

4. Dane osobowe poza zasięgiem AI

Jeśli AI nie musi widzieć nazwisk czy numerów, maskujemy je, zanim dane trafią do modelu.

5. Hasła w sejfie

Hasła i klucze dostępne przechowujemy w zaszyfrowanym sejfie, osobno dla każdego klienta. Nigdy nie trafiają do maili ani do kodu.

6. Treści z zewnątrz to tylko dane

Maile, strony i załączniki od obcych osób nie mogą wydawać poleceń systemowi. Zabezpieczamy go przed próbami manipulacji.

7. Pełny rejestr działań

Każde działanie systemu jest zapisywane. Zawsze wiadomo, co, kiedy i na czyje polecenie się wydarzyło.

8. Kopie zapasowe

Dane mają automatyczną kopię zapasową, a zmiany da się cofnąć. Awaria nie oznacza utraty danych.

9. Czyste zakończenie

Po zakończeniu współpracy odbieramy sobie wszystkie dostępności i usuwamy dane. Potwierdzamy to na piśmie.

Gdzie są Państwa dane — decydują Państwo

Chmura w UE

Dane przechowywane i przetwarzane na serwerach w Unii Europejskiej. Najszybsze wdrożenie.

Wariant mieszany

Dane pozostają w firmie. Do zewnętrznego AI trafia tylko to, co niezbędne, bez danych osobowych.

Całkowicie lokalnie

Baza i model AI na serwerze w Państwa firmie. Dla danych, które nie mogą opuścić budynku.

Formalności

- **Umowa powierzenia przetwarzania danych** (RODO art. 28) podpisywana razem z umową główną, z listą podmiotów przetwarzających dane.
- **Przejrzystość wobec klientów:** asystenci głosowi i czatowi informują, że rozmówca rozmawia z AI (wymóg AI Act).
- **Ocena dostawców:** firmom objętym nową ustawą o cyberbezpieczeństwie (NIS2) przekazujemy informacje potrzebne do oceny nas jako dostawcy.

Czego nie obiecujemy: stuprocentowego bezpieczeństwa. Tego nie może uczciwie zagwarantować nikt. Obiecujemy, że ryzyko jest ograniczone do minimum, a każda z powyższych zasad jest sprawdzalna.