Dane bez twarzy

Autorzy: zespół “Nazwa drużyny”

Problem: bezpieczne wykorzystanie danych tekstowych

- **Rodzaje danych w tekstach użytkowych:** Maile, czaty, logi, notatki medyczne czy HR oraz ankiety zawierają dane osobowe (PESEL, numery dokumentów, konta bankowe, kontakty) oraz informacje wrażliwe (zdrowie, poglądy polityczne, religia).
- **Ryzyko prawne i bezpieczeństwa:** Wykorzystanie takich danych bez odpowiedniego przetwarzania narusza RODO, grozi wyciekiem informacji oraz złamaniem wewnętrznych polityk bezpieczeństwa.
- **Ograniczenia prostych metod anonimizacji:** Proste regexy nie wykrywają kontekstu (np. zdrowie), są nieskuteczne dla języka polskiego i trudne do skalowania.
- **Wymagania organizacji:** Firmy potrzebują rozwiązań redukujących ryzyko ujawnienia danych, zachowujących przy tym wartość analityczną tekstu i możliwych do łatwej integracji jako API.

Source: https://star.edu.pl/rodo-co-to

Rozwiązanie: Kontekstowa anonimizacja tekstu

Kontekstowe rozpoznawanie danych wrażliwych
Model językowy analizuje kontekst zdania i wykrywa dane osobowe oraz informacje wrażliwe (np. zdrowie, poglądy), nawet bez jednoznacznych wzorców.

Obsługa języka polskiego
System dostosowany do zawiłości języka polskiego – rozpoznaje odmiany, skróty, różne sposoby zapisu danych.

Zachowanie treści analitycznej
Po anonimizacji tekst zachowuje strukturę i znaczenie – nadaje się do analizy i wykorzystania w AI.

Rozwiązanie

- **Wykrywanie twardych identyfikatorów:** PESEL, numery telefonów, konta bankowe, e-maile i dokumenty są wykrywane za pomocą precyzyjnych reguł dopasowanych do polskich danych.
- **Wykrywanie formy gramatycznej:** Morfeusz2 pozwala nam zachowywać formę gramatyczną wrażliwych danych żebyśmy mogli generować poprawne zamienniki
- **Technologie:** Python + Flask (API i UI), Morfeusz2 (morfologia), Docker (łatwa integracja i deployment).

Podsumowanie

- Wykrywanie danych za pomocą samych regexów i Morfeusza oferuje dość szybkie choć mocno ograniczoną funkcjonalność, zwłaszcza dla danych bazujących na kontekście.
- Można je rozbudować poprzez dodanie anonimizacji za pomocą LLM po wstępnej tokenizacji.