



Zastępca Prezydenta Miasta Szczecin

Michał Przepiera

pl. Armii Krajowej 1, 70-456 Szczecin

tel. +4891 43 51 100, fax +4891 42 30 806

mprzepie@um.szczecin.pl • www.szczecin.eu

Szanowny Pan
Dariusz Smoliński
Radny Miasta Szczecin

Znak sprawy: WZP-I.0003.1.2026.Psz

Dotyczy: Interpelacja nr 1718

W nawiązaniu do interpelacji dotyczącej wdrożenia projektu pilotażowego pn. „Contact Center v1” w Urzędzie Miasta Szczecin, poniżej zamieszczam odpowiedzi na postawione pytania:

1. W ramach etapu pilotażowego oraz w kolejnych etapach wdrażania systemu działaniem systemu zostanie objętych ok. 558 spraw i procedur Urzędu Miasta Szczecin, których lista znajduje się na stronie [www: https://eurzad.szczecin.pl/chapter_51199.asp](https://eurzad.szczecin.pl/chapter_51199.asp).
2. Poprawność, aktualność oraz kontrola jakości udzielanych przez system odpowiedzi została zapewniona poprzez zastosowanie technologii RAG (Retrieval - Augmented Generation), która łączy możliwości zaawansowanego modelu językowego z dostępem do zewnętrznych baz wiedzy (w tym przypadku bazy Urzędu Miasta Szczecin). Dzięki zastosowaniu RAG, sztuczna inteligencja nie uczy się procedur na pamięć, lecz każdorazowo przeszukuje specjalnie przygotowaną, lokalną bazę danych opartą na aktualnych treściach (portal: eurzad.szczecin.pl). Kontrola jakości odbywa się poprzez procedurę testową zawierającą specjalnie przygotowany zestaw pytań. Odpowiedzi udzielane przez chatbota są oceniane w kilku kategoriach, a każdorazowa zmiana jego konfiguracji jest oceniana przez powtarzalny proces testów przeprowadzanych przez pracowników Biura Obsługi Interesantów Urzędu Miasta Szczecin. Po upublicznieniu systemu planowany jest okres testów z mieszkańcami pozwalający na ocenę jakości udzielanych odpowiedzi, co umożliwi zwiększenie skuteczności i przydatności Contact Center v1.
3. W celu ochrony danych osobowych oraz zapewnienia zgodności systemu z przepisami RODO zastosowano następujące rozwiązania:
 - a) w ramach projektu przygotowano kartę DPIA zawierającą analizę ryzyk związanych z ochroną danych,
 - b) ścisły zakaz wprowadzania danych osobowych (PII) przez testerów; dopuszczalne są jedynie dane syntetyczne,

- c) do bazy danych (RAG) chatbota przekazywane są wyłącznie informacje publiczne (Procedury Urzędu Miasta Szczecin),
 - d) komunikacja na zewnątrz infrastruktury Urzędu Miasta Szczecin odbywa się wyłącznie poprzez szyfrowane protokoły danych,
 - e) wdrożono politykę Zero Data Retention – zgodnie z licencjami wykorzystywanych modeli LLM dane z zapytań API nie są wykorzystywane do trenowania modeli publicznych,
 - f) administratorzy mają wgląd w logi audytowe, aby weryfikować przestrzeganie procedur bezpieczeństwa.
4. Niezależność systemu od jednego dostawcy została osiągnięta poprzez stworzenie przez Wykonawcę środowiska AI, które umożliwia wykorzystywanie różnych modeli dostawców LLM. Do tego celu zostały dostosowane elementy systemu (języki programowania, frameworki, systemy baz danych, biblioteki front-end i back-end oraz aplikacje połączone za pośrednictwem interfejsów API). W okresie testów wykorzystywane będą modele firm Google oraz Open AI ale w każdej chwili mogą one zostać zastąpione innymi rozwiązaniami np. Bielik, PLLuM lub inne.
5. W aktualnej architekturze środowisko AI w tym baza RAG i logika biznesowa całego systemu znajduje się na lokalnych serwerach Urzędu Miasta o minimalnej konfiguracji: 2-4 GB RAM i 2-4 vCPU, Przetwarzanie odpowiedzi LLM (Large Language Model) odbywa się w komercyjnej chmurze - w zależności od wykorzystywanego modelu aktualnie jest to chmura Google lub Open AI.

W ramach projektu nie będą wykorzystywane komercyjne usługi przetwarzania danych. Bot AI będzie udzielał odpowiedzi wyłącznie na podstawie treści publicznych, co powoduje brak konieczności przetwarzania danych osobowych.

ZASTĘPCA PREZYDENTA MIASTA
Michał Przepiera