

1. Które z dostępnych obecnie aplikacji (ChatGPT, Gemini, Perplexity, Claude, Mistral, Copilot, Notebook LM itd.) są polecane dla administracji publicznej?

Administracja publiczna powinna — w mojej ocenie — opierać większość zadań administracyjnych na modelach lokalnych (takich jak Bielik, PLLuM czy Gemma 4) skonfigurowanych z lokalnymi aplikacjami klasy Anything LLM lub Open WebUI. To podejście zapewnia najwyższy poziom bezpieczeństwa danych, wymaga jednak inwestycji w serwery o odpowiedniej mocy obliczeniowej.

Rozwiązaniem komplementarnym są platformy zewnętrznych dostawców — pod warunkiem korzystania z subskrypcji enterprise, która wiąże podmiot publiczny z dostawcą umową o przetwarzaniu danych (DPA). Warto zaznaczyć, że w ramach tych umów często obowiązuje również wymóg rezydencji danych na terenie Europy.

Opcją minimum pozostają plany Pro, jednak ich wdrożenie musi być poprzedzone dwoma krokami: zapewnieniem pracownikom narzędzi do anonimizacji danych oraz opracowaniem przejrzystych procedur określających, jakie kategorie danych i do jakich celów mogą być przetwarzane z wykorzystaniem tych narzędzi.

Jeśli chodzi o konkretne rekomendacje narzędziowe — na dziś wskazałbym **Claude** ze względu na dojrzałą funkcjonalność agentową (Cowork) oraz **Gemini** za multimodalność i szerokość zastosowań.

2. Jakie jedno zastosowanie AI w administracji publicznej już dziś przynosi mierzalny efekt (czas, koszt, jakość) i jakie są na to twarde dane?

Zacznę od uczciwego zastrzeżenia metodologicznego: podstawowy problem administracji publicznej polega na tym, że instytucje rzadko mierzą wskaźniki sukcesu wdrożonych rozwiązań. Brakuje systematycznych, porównywalnych danych — co samo w sobie jest diagnozą dojrzałości cyfrowej sektora.

Z własnych doświadczeń projektowych oraz dostępnych danych wskazałbym automatyzację sprawozdawczości i raportowania jako obszar, gdzie mierzalny efekt pojawia się najszybciej i najwyraźniej.

Zastosowanie AI do przygotowywania raportów, sprawozdań i dokumentacji urzędowej pozwala skrócić czas ich przygotowania o **60–70%**. Dlaczego akurat sprawozdawczość? Bo efekt jest natychmiast mierzalny (czas przed/po), nie wymaga zmiany procesów decyzyjnych, a ryzyko błędu jest łatwe do kontroli przez człowieka. To najniżej wiszący owoc — i dobry punkt startowy dla instytucji, które chcą zbudować wewnętrzne przekonanie do AI, zanim sięgną po bardziej złożone zastosowania.

3. Jakie narzędzie AI do pracy w administracji publicznej rekomendujecie Państwo, mowa o analizie dokumentów, automatyzacji pracy?

Warto rozdzielić te dwa zastosowania, bo wymagają różnych podejść.

Analiza dokumentów — tutaj rekomendujemy modele lokalne: Bielik lub PLLuM, skonfigurowane w architekturze RAG (Retrieval-Augmented Generation) lub włączone w workflow agentowy. Modele te działają w zamkniętym środowisku, co eliminuje ryzyko wycieku danych, a jednocześnie są zoptymalizowane pod język polski i specyfikę dokumentów administracyjnych. RAG pozwala „rozmawiać” z dokumentami bez konieczności ich wysyłania do zewnętrznych serwerów.

Automatyzacja pracy — tu odpowiedź zależy od tego, z jakimi danymi pracujemy. Jeśli operujemy na danych otwartych lub zanonimizowanych, dobrze sprawdza się **Claude** — szczególnie w kontekście pracy agentowej i automatyzacji złożonych zadań biurowych. W środowisku zamkniętym, gdzie dane nie mogą opuszczać infrastruktury instytucji, polecamy **n8n** jako platformę do budowania przepływów automatyzacji — open-source, możliwy do hostowania lokalnie, z szerokim ekosystemem integracji.

Niezależnie od narzędzia, kluczowe jest wcześniejsze opracowanie procedur określających, które dane mogą być przetwarzane przez które narzędzia — bez tego nawet najlepiej dobrane oprogramowanie staje się ryzykiem, a nie zasobem.

4. Czy dobrym rozwiązaniem jest żądanie od Chata podawania zawsze źródeł, z których korzysta — do weryfikacji poprawności odpowiedzi? Jakie są zagrożenia takiego rozwiązania?

Jest to dobra metoda, ale często się zdarza, że podane źródła nie istnieją (po kliknięciu w link) lub chat czerpie z niewielkiej części tych źródeł informacji, co wpływa na zniekształcenie wyników. Polecam przejrzeć wyniki tego badania. Pokazuje ono, jak narzędzia ai mimo powoływania się na źródła, potrafią halucynować: https://www.cjr.org/tow_center/we-compared-eight-ai-search-engines-theyre-all-bad-at-citing-news.php

5. Czy przy płatnych modelach AI również trzeba przed wrzuceniem dokumentów anonimizować samemu dane czy AI robi to za nas?

Tak — przy standardowych planach płatnych (np. Pro) anonimizacja leży po stronie użytkownika. Łączy nas z dostawcą wyłącznie umowa subskrypcyjna, a dane są przetwarzane na serwerach zagranicznych, najczęściej w USA. Dostawca nie gwarantuje w takim modelu ani ochrony danych zgodnej z RODO, ani tego, że dane nie trafią do procesu trenowania modelu.

Dopiero subskrypcja enterprise zmienia ten układ — umowa jest wówczas uzupełniona o DPA (Data Processing Agreement), czyli umowę o przetwarzaniu danych osobowych wymaganą przez RODO. W jej ramach dostawca zobowiązuje się do określonych standardów bezpieczeństwa, często oferuje rezydencję danych na terenie UE oraz gwarantuje, że dane nie są wykorzystywane do trenowania modeli.

6. Który model najlepiej sprawdzi się do napisania protokołu z sesji Rady Miasta? Czy AI jest w stanie stworzyć transkrypcję, po wklejeniu linku z nagrania sesji Rady Miasta (nagranie jest z napisami)?

Do transkrypcji najlepiej wykorzystać albo whisper (darmowy) albo rozwiązanie polskie stenograf: <https://stenograf.io/>, kwestia przypisania mówców najlepiej, żeby należała do człowieka. Z kolei z gotową transkrypcją protokół można przygotować w dobrej jakości w Claude Cowork podobnie, jak pokazałem na tutorialu.

7. Jakie narzędzie użył Pan jako "anonimizatora"? Czy to była aplikacja lokalna? Na jakiej zasadzie działa pokazany podczas prezentacji anonimizator? Wyszukuje dane osobowe na podstawie nazw kolumn w pliku czy na podstawie innego algorytmu? Czy to narzędzie jest ogólnodostępne?

Anonimizator, który pokazałem, to jest nasze prywatne rozwiązanie. Planujemy udostępnić je za darmo. Na razie repozytorium kodu tego rozwiązania znajduje się na naszym koncie na github: <https://github.com/radlab-dev-group/omni-mask>. W ciągu 3-4 tygodni udostępnimy pod tym adresem darmową aplikację open source do anonimizacji danych.

8. Które modele mają możliwości agentowe?

Moim zdaniem najłatwiej opanować agentów w Claude (Cowork lub Claude Code) i Antigravity (Google).

9. Przygotowanie odpowiednich baz danych pod AI. Jak powinna wyglądać struktura w organizacji, aby efektywnie zarządzać AI?

To złożone pytanie, które warto rozdzielić na dwa poziomy.

Poziom techniczny

Administracja publiczna dysponuje ogromnym zasobem dokumentów, ale rzadko są one gotowe do efektywnego wykorzystania przez AI. Żeby architektura RAG (czyli

„rozmawianie” z dokumentami) działała skutecznie, potrzebne są trzy rzeczy: porządek, jakość i aktualność.

Jeśli chodzi o formaty plików — nie wszystkie są równie przyjazne dla AI. Najlepiej działają dokumenty tekstowe: TXT, Markdown, DOCX oraz PDF z warstwą tekstową (czyli nie skany). Problematiczne są zeskanowane PDFy bez OCR, stare formaty DOC oraz dokumenty z rozbudowanymi tabelami graficznymi — AI ma trudność z ich poprawną interpretacją. Dane ustrukturyzowane, takie jak rejestry czy ewidencje, najlepiej przechowywać w formacie CSV lub JSON, które są natywnie czytelne dla systemów AI.

Równie ważne jak format jest miejsce przechowywania. W polskiej administracji najczęściej funkcjonują systemy klasy EKD (Elektroniczne Zarządzanie Dokumentacją) — jeśli instytucja z nich korzysta, to właśnie tam powinna budować uporządkowane zasoby dokumentów. W organizacjach pracujących na środowisku Microsoft dobrze sprawdza się SharePoint jako repozytorium wiedzy zasilające narzędzia AI. Do bardziej zaawansowanych wdrożeń RAG, gdzie dokumenty są indeksowane i przeszukiwane przez model, stosuje się dedykowane bazy wektorowe — np. Chroma, Qdrant lub pgvector — które przechowują dokumenty w formie zrozumiałej dla modeli językowych.

Najczęstszy problem nie jest jednak techniczny, lecz proceduralny: instytucje gromadzą dokumenty latami bez żadnej polityki retencji, co sprawia, że model „uczy się” na przestarzałych lub sprzecznych informacjach.

Poziom organizacyjny

Tu administracja publiczna stoi przed realnym wyzwaniem, bo większość jednostek — szczególnie JST — nie ma zasobów kadrowych, by tworzyć dedykowane zespoły AI. Proponuję myśleć o tym przez pryzmat trzech ról, niekoniecznie trzech etatów:

- Koordynator AI — osoba odpowiedzialna za politykę używania narzędzi AI, aktualizację procedur i kontakt z dostawcami. W małej jednostce może to być pracownik IT lub pełnomocnik ds. cyfryzacji z rozszerzonym zakresem zadań.
- Opiekun danych (data steward) — osoba w każdym wydziale odpowiedzialna za jakość i aktualność dokumentów zasilających systemy AI. To rola procesowa, nie techniczna.

- Użytkownik przeszkolony — każdy pracownik korzystający z narzędzi AI powinien przejść szkolenie z zakresu tego, co można, a czego nie można przetwarzać, oraz jak weryfikować wyniki.

Kluczowa zasada pozostaje niezmienna: AI nie działa lepiej niż dane, na których pracuje, i nie zarządza się sama. Brak struktury organizacyjnej wokół AI to nie oszczędność — to odroczony koszt błędów i ryzyk prawnych.

10. Jakie są trzy najczęstsze błędy administracji publicznej przy wdrażaniu AI?

Po pierwsze zły wybór procesów. Urzędy często próbują zacząć od procesów złożonych, wyjątkowych i niestandardizowanych. Tymczasem AI działa najlepiej tam, gdzie zadania są powtarzalne i dobrze zdefiniowane.

Po drugie brak polityki danych przed wdrożeniem. Narzędzia są wdrażane bez odpowiedzi na fundamentalne pytania: jakie dane mogą być przetwarzane, przez kogo i gdzie. Efekt: pracownicy albo nie używają AI wcale z obawy przed błędem, albo używają niezgodnie z RODO — i obie sytuacje są złe.

Po trzecie traktowanie AI jako projektu IT, nie zmiany organizacyjnej. Kupuje się narzędzie, wdraża technicznie i oczekuje efektów. Bez szkoleń, bez procedur, bez mierzenia wyników. AI nie przynosi wartości przez sam fakt istnienia — wymaga zmiany nawyków pracy i świadomego zarządzania.

11. Czy pod wdrożenie AI w urzędzie wymagany jest zakup sprzętu, czy są inne alternatywy bezkosztowe?

Jeśli urząd pracuje na danych ogólnodostępnych lub zanonimizowanych, może korzystać z narzędzi chmurowych bez żadnej inwestycji w infrastrukturę. Bezpłatne lub niskokosztowe opcje to m.in. Claude, ChatGPT, Gemini czy Microsoft Copilot. Warto przy tym sprawdzić, czy instytucja posiada już licencję **Microsoft 365** — wiele JST ją ma,

a aktywacja Copilota nie wymaga zakupu nowego sprzętu, tylko rozszerzenia istniejącej subskrypcji. To często najbliższy leżący owoc, który jest pomijany.

W tym modelu koszt jest zerowy lub sprowadza się do subskrypcji miesięcznej, a wdrożenie może nastąpić w ciągu dni, nie miesięcy.

Jeśli urząd chce przetwarzać przez AI dane wrażliwe, osobowe lub niejawne — bez ryzyka ich wysyłania poza własną infrastrukturę — konieczne jest uruchomienie modelu lokalnie.

Warto rozważyć dwa rozwiązania, które obniżają próg wejścia:

- Subskrypcja enterprise u zewnętrznego dostawcy — dane przetwarzane są w chmurze, ale objęte umową DPA i często rezydencją w UE. Koszt subskrypcji, bez inwestycji w sprzęt.
- Infrastruktura współdzielona — niektóre regiony i związki JST budują wspólne centra przetwarzania danych. To model, który pozwala rozłożyć koszty sprzętowe między kilka jednostek.

12. Czy planowana jest "systemowa konstytucja wykorzystania AI w JST"

określająca warunki wykorzystania nowych narzędzi w samorządach?

Myślę, że nie. Każdy urząd musi określić swoje standardy wykorzystania AI np: Warszawa zaczęła od

kodeksu: https://um.warszawa.pl/documents/114265126/0/PL_WARSZAWSKI+KODEKS+GenAI_241128.pdf/b9a7bc92-48aa-6042-3601-624722682d6b?t=1742992739220

13. Czy można dokładnie wskazać strukturę dokumentu, który ma utworzyć AI

(rodzaj szablonu)?

Tak można. Możemy ją opisać dokładnie modelowi albo pokazać przykład szablonu, na którym nam zależy.

14. AI a RODO - Jak wiemy większość modeli Sztucznej Inteligencji otrzymywane od nas dane przekazuje swoim twórcom. Jak wobec tego ma się RODO? Jakie obostrzenia powinien wprowadzić Inspektor Danych Osobowych naszego urzędu?

Czy narzędzia AI w administracji publicznej mogą być dobrym rozwiązaniem do wskazywania, które dane powinny być anonimizowane w dokumentach urzędowych oraz czy ich zastosowanie zależy od wewnętrznej polityki wprowadzonej przez Inspektora Ochrony Danych (IOD)? Jeżeli tak, to z jakiego narzędzia AI, wymienionych w prezentacji skorzystać, aby była skuteczna? (odpowiedź na obydwa pytania):

Zacznijmy od precyzji: modele AI nie „kradną” danych osobowych — jednak każdorazowe przestanie zapytania do zewnętrznego serwisu oznacza przekazanie danych do przetwarzania przez podmiot trzeci, co w świetle RODO rodzi konkretne obowiązki prawne.

Jeśli urząd korzysta z bezpłatnej lub standardowej wersji płatnej narzędzia AI, najczęściej nie istnieje żadna umowa o przetwarzaniu danych osobowych (DPA/UPD). Dane trafiają na serwery dostawcy — zazwyczaj w USA — bez gwarancji zgodności z RODO. Dostawcy w wersjach płatnych (Pro) deklarują co prawda, że nie trenują modeli na danych użytkowników, ale deklaracja to nie umowa, a transfer danych poza EOG i tak następuje. Dopiero subskrypcja enterprise zmienia ten stan rzeczy: urząd zawiera z dostawcą umowę DPA wymaganą przez art. 28 RODO, często z klauzulami dotyczącymi rezydencji danych w UE. Alternatywą eliminującą transfer całkowicie są modele lokalne — dane nie opuszczają infrastruktury instytucji.

Co powinien zrobić Inspektor Ochrony Danych?

IOD powinien wyjść od analizy ryzyka i przełożyć ją na konkretne procedury. W praktyce oznacza to co najmniej pięć działań:

Pierwsza sprawa to klasyfikacja danych. IOD powinien opracować matrycę określającą, które kategorie danych mogą być przetwarzane przez AI, a które są wykluczone. Dane

osobowe zwykłe, dane wrażliwe (art. 9 RODO) np: dane dotyczące postępowań administracyjnych czy dane dzieci wymagają różnych poziomów ostrożności.

Druga to lista dopuszczonych narzędzi wraz z warunkami użycia — z rozróżnieniem: to narzędzie można stosować do danych zanonimizowanych, tamto wyłącznie po podpisaniu DPA, a lokalne modele bez ograniczeń co do kategorii danych.

Trzecia to procedura anonimizacji i pseudonimizacji — pracownicy muszą wiedzieć nie tylko że mają anonimizować dane, ale *jak* to robić poprawnie. Sama zamiana imienia na inicjały nie spełnia standardów anonimizacji w rozumieniu RODO.

Czwarta to obowiązek przeprowadzenia DPIA przed uruchomieniem każdego nowego zastosowania AI, które przetwarza dane osobowe na większą skalę lub dotyczy danych wrażliwych.

Piąta to szkolenie pracowników — procedury bez kompetencji nie działają. Każdy użytkownik narzędzi AI powinien przejść szkolenie z zakresu dozwolonych praktyk i wiedzieć, do kogo zgłosić incydent.

IOD nie powinien zakazywać AI — powinien ją ucywilizować. Zbyt restrykcyjne podejście wypycha pracowników w stronę niekontrolowanego używania prywatnych kont i narzędzi, co generuje większe ryzyko niż wdrożenie z jasnymi zasadami.

15. Jakie kompetencje w zakresie AI są najbardziej pożądane u osób

zaangażowanych we wdrożenia AI w administracji publicznej, ale nienależących do działów informatycznych? Które z nich mają kluczowe znaczenie na etapie planowania i zarządzania zmianą?

Najważniejsza umiejętność to zdolność do rozkładania złożonych zadań administracyjnych na mniejsze, powtarzalne kroki — i oceny, które z nich nadają się do wsparcia przez AI, a które wymagają ludzkiej decyzji. To właśnie tu leży największa luka kompetencyjna w urzędach: pracownicy albo nie widzą potencjału automatyzacji w swojej codziennej pracy, albo oczekują od AI zbyt wiele.

Z tą umiejętnością nierozłącznie wiąże się zdolność przekładania istniejących procedur na wersje z AI — czyli nie projektowanie od zera, lecz reengineering tego, co już istnieje.

Osoba, która rozumie procedury urzędu i jednocześnie rozumie, co AI potrafi, a czego nie, jest w organizacji więcej warta niż najlepszy programista.

Poza myśleniem procesowym kluczowe są:

- Prompt engineering i krytyczna ocena wyników AI
- Świadomość prawna i danych osobowych.

Na etapie wdrożenia największy opór pochodzi nie z braku technologii, lecz z lęku i niezrozumienia. Osoba koordynująca wdrożenie musi umieć tłumaczyć cele zmiany językiem korzyści dla konkretnych zespołów, a nie językiem technologii. To kompetencja miękka o twardym wpływie na powodzenie projektu.