

ZARZĄDZENIE NR 369/ 2026
PREZYDENTA MIASTA SUWAŁK

z dnia 13 października 2026 r.

w sprawie wdrożenia Polityki Bezpiecznego Stosowania Systemów Sztucznej Inteligencji (AI)
w Urzędzie Miejskim w Suwałkach

Na podstawie art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2026 r. poz. 662) , w związku z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) oraz ustawą z dnia 3 lipca 2026 r. o systemach sztucznej inteligencji (Dz. U. z 2026 r. poz.1003), zarządzam, co następuje:

§ 1. 1. W celu zapewnienia wysokich standardów bezpieczeństwa informacji, ochrony danych osobowych, a także praw i wolności obywateli przy jednoczesnym wspieraniu bezpiecznej innowacyjności, wdraża się w Urzędzie Miejskim w Suwałkach Politykę Bezpiecznego Stosowania Systemów Sztucznej Inteligencji (AI).

2. Polityka, o której mowa w ust. 1, stanowi Załącznik do niniejszego zarządzenia i jest wiążąca dla wszystkich pracowników Urzędu Miejskiego w Suwałkach w zakresie wykonywanych przez nich obowiązków służbowych.

§ 2. Zobowiązuje się naczelników wydziałów, kierowników referatów oraz pracowników do zapoznania się z treścią zarządzenia, stosowania oraz do bieżącej weryfikacji wykorzystywanych w pracy narzędzi AI pod kątem ich zgodności ze standardami bezpiecznego stosowania w realizacji powierzonych zadań.

§ 3. Nadzór nad wykonaniem niniejszego zarządzenia powierza się Sekretarzowi Miasta.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta Suwałk

Czesław Renkiewicz

Polityka Bezpiecznego Stosowania Systemów Sztucznej Inteligencji

§ 1. 1. Celem niniejszej polityki jest zapewnienie zgodnego z prawem, etycznego i przejrzystego stosowania systemów sztucznej inteligencji (AI) w Urzędzie Miejskim w Suwałkach, minimalizującego ryzyko naruszenia przepisów prawa ogólnie obowiązującego, uregulowań wewnętrznych urzędu w szczególności w zakresie ochrony danych osobowych i ochrony informacji.

2. W celu skoordynowania stosowania narzędzi sztucznej inteligencji (AI) powołuje się Koordynatora ds. wykorzystywania AI w Urzędzie Miejskim w Suwałkach, zwanego dalej koordynatorem ds. AI

§ 2. Ilekróć w niniejszym zarządzeniu jest mowa o:

- 1) Urzędzie lub jednostce – należy przez to rozumieć Urząd Miejski w Suwałkach;
- 2) Komórce organizacyjnej Urzędu należy przez to rozumieć wydział, referat, biuro, samodzielne stanowiska pracy;
- 3) Kierownik komórki organizacyjnej – należy przez to rozumieć naczelnika wydziału, kierownika wydziału, referatu, biura urzędu, samodzielne stanowisko pracy.
- 4) AI Act lub Akt o AI- należy przez to rozumieć rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji)

§ 3. 1. Zobowiązuje się Koordynatora ds. AI do prowadzenia Rejestru Wdrożonych Systemów Sztucznej Inteligencji wykorzystywanych w Urzędzie.

2. Każde planowane projektowanie i wdrożenie do użycia systemowego narzędzia AI wymaga uprzedniego zgłoszenia i przypisania do jednej z kategorii ryzyka:

- 1) Wysokie ryzyko (wymagające szczególnego nadzoru);
- 2) Niskie ryzyko (podlegające ogólnym zasadom przejrzystości);
- 3) Minimalne ryzyko (narzędzia technicznego wykorzystania: autokorekta tekstu, analiza danych wewnętrznych, narzędzie do streszczania, filtrowanie spamu, itp.).

§ 4. W Urzędzie zabrania się wdrażania i używania niedozwolonych systemów oraz otwartych narzędzi AI, które:

- 1) Analizują lub rozpoznają emocje osób i pracowników przebywających na terenie Urzędu;
- 2) Służą do profilowania i oceny behawioralnej osób (scoring społeczny);
- 3) Wykorzystują techniki podprogowe lub manipulacyjne w celu wymuszenia podjęcia określonych decyzji;
- 4) Wykorzystują „słabość” określonej grupy osób ze względu na ich wiek, niepełnosprawność lub szczególną sytuację społeczną lub ekonomiczną;
- 5) Dokonują biometrycznej kategoryzacji osób według cech wrażliwych lub identyfikacji biometrycznej w czasie rzeczywistym i tworzenia baz rozpoznawania twarzy.

§ 5. W przypadku korzystania przez pracowników z otwartych systemów generatywnej sztucznej inteligencji wprowadza się następujące zasady:

- 1) Zasada minimalizacji danych: oznacza bezwzględny zakaz wprowadzania do zewnętrznych, otwartych narzędzi i systemów AI danych osobowych (zgodnie z RODO), informacji niejawnych, tajemnic skarbowych, danych finansowo-księgowych Urzędu, wewnętrznych dokumentów urzędu i innych danych prawnie chronionych;
- 2) Zasada ograniczonego zaufania: każda treść wygenerowana przez AI (tekst, kod źródłowy, analiza, itp.) musi zostać zweryfikowana merytorycznie przez pracownika merytorycznego przed publikacją lub wysłaniem. AI w tym zakresie pełni wyłącznie funkcję pomocniczą;
- 3) Obowiązuje bezwzględny zakaz przygotowywania przez AI ostatecznych treści decyzji administracyjnych, stosowania AI do maszynowego podejmowania decyzji i tworzenia ich treści, które następnie są podpisywane przez osoby upoważnione do ich wydawania – ostateczne rozstrzygnięcie zawsze podejmowane jest przez upoważnionego pracownika urzędu;
- 4) Prawa autorskie: zabrania się wykorzystywania AI do generowania oficjalnych dokumentów zewnętrznych bez oznaczenia faktu użycia algorytmu, jeśli system generuje treści mogące wprowadzać w błąd, co do tożsamości autora.

§ 6. 1. W przypadku wdrożenia systemów AI wchodzących w bezpośrednią interakcję z mieszkańcami (np. chatboty, voiceboty), system musi w sposób jasny i czytelny informować użytkownika, że komunikuje się ze sztuczną inteligencją.

2. Mieszkaniec ma prawo zażądać, aby jego sprawa obsługiwana automatycznie przez algorytm została przekierowana do prowadzenia przez pracownika Urzędu.

§ 7. 1. Zobowiązuje się osoby zatrudnione w Urzędzie do:

- 1) złożenia oświadczenia, którego wzór stanowi załącznik do niniejszej polityki, o zapoznaniu się z Polityką Bezpiecznego Stosowania Systemów Sztucznej Inteligencji (AI);
- 2) udziału w szkoleniu wprowadzającym do bezpiecznego użytkowania systemów AI;
- 3) zapoznania się z „Przewodnikiem po sztucznej inteligencji dla administracji publicznej” wydanym przez Ministerstwo Cyfryzacji RP.

2. Zobowiązuje się Wydział Organizacyjny do organizowania regularnych szkoleń z zakresu bezpiecznego użytkowania AI, ryzyk związanych z halucynacjami algorytmów oraz ochrony prywatności.

§ 8. Pracownicy Urzędu zobowiązani są do stosowania zaleceń bezpiecznego promptowania:

- 1) Do publicznych i ogólnodostępnych modeli AI (np. ChatGPT, Claude, Copilot) nigdy nie wprowadzamy danych osobowych osób ani konkretnych spraw urzędowych. Zamiast tego stosujemy generalizację (uogólnianie) i fikcyjne dane personalne;
- 2) Jeśli zadaniem AI jest streszczenie dokumentu, poprawa błędów stylistycznych lub wyciągnięcie wniosku z raportu, należy go odpowiednio przygotować (np. zabezpieczyć dane wrażliwe, osobowe itp.);
- 3) Architektura Bezpiecznego Promptu Samorządowego (Model 4X):
 - a) Rola (Kim jest AI): Należy przypisać AI rolę w jakiej ma pracować, np.: rola pracownika samorządowego,
 - b) Kontekst (Co robisz): Należy opisać ogólną sytuację bez szczegółów wrażliwych,
 - c) Zadanie (Czego oczekujesz): Należy określić precyzyjne polecenie działania,
 - d) Ograniczenie (Czego AI NIE wolno robić): Kluczowe dla bezpieczeństwa prawnego. Należy podać, aby AI nie dodawał od siebie żadnych nowych faktów, procedur ani interpretacji prawnych, które nie wynikają z tekstu źródłowego lub wskazanych w prompcie obowiązujących aktów prawnych.

4) Lista kontrolna przed kliknięciem „Wyślij” (Wyślij / Cofnij)

Zanim pracownik zatwierdzi zapytanie w oknie chatu AI, musi sprawdzić:

- a) Czy w tekście nie znajduje się nazwisko, adres, PESEL, numer rejestracyjny lub nr telefonu,
- b) Czy informacje wprowadzone do promta, są jawne lub publicznie dostępne (np. wewnętrzne notatki, projekty budżetu przed publikacją),
- c) Czy model, z którego korzystam, nie zapisuje moich danych do trenowania? (W darmowych wersjach zawsze zakładaj, że dane są zapisywane i mogą trafić do Internetu),
- d) Każdy przepis prawny, artykuł, czy termin przytoczony przez AI musi zostać sprawdzony przez osobę korzystającą z AI w dostępnej bazie aktów prawnych.

§ 9. 1. Wprowadza się obowiązkową procedurę przedwdrozeniowej oceny zgodności dla każdego nowego systemu sztucznej inteligencji, który Urząd zamierza zakupić w drodze zamówień publicznych, pozyskać w ramach darmowych licencji lub testów, stworzyć wewnętrznie na potrzeby Urzędu lub jednostek podległych.

2. Każda komórka organizacyjna Urzędu przed wszczęciem procedury zakupowej systemu zawierającego elementy AI jest zobowiązana do złożenia wniosku do Koordynatora ds. AI. Wniosek musi zawierać:

- 1) Opis celu stosowania i przeznaczenia systemu;
- 2) Deklarację dostawcy oprogramowania dotyczącą poziomu ryzyka systemu według AI Act;
- 3) Informację, czy system będzie przetwarzał dane osobowe mieszkańców (wymaga opinii Inspektora Ochrony Danych).

3. Zabrania się zakupu i wdrażania systemów AI bez uzyskania pisemnej akceptacji zgodności z AI ACT wydanej przez Koordynatora ds. AI oraz przez Inspektora Ochrony Danych- w sprawach dotyczących danych osobowych lub radcę prawnego- w zakresie wymagającym oceny prawnej.

4. W zapytaniach ofertowych oraz Specyfikacji Warunków Zamówienia (SWZ) dotyczących systemów IT zawierających AI, Urząd ma obowiązek wymagać od wykonawców:

- 1) Przekazania pełnej, zrozumiałej instrukcji obsługi w języku polskim, umożliwiającej nadzór człowieka nad systemem AI;
- 2) Gwarancji i certyfikatów zgodności z wymogami Aktu o AI, w szczególności dla systemów wysokiego ryzyka;
- 3) Wglądu do dokumentacji technicznej, o której mowa w art. 11 ust. 1 AI ACT;
- 4) Wykazania, że model AI nie był trenowany z naruszeniem praw autorskich;
- 5) Każde nowe, zatwierdzone narzędzie AI przed udostępnieniem pracownikom musi zostać wpisane do Rejestru Systemów AI Urzędu, o którym mowa w § 3 niniejszego Polityki.

§ 10. 1. Każdy system AI przed ostatecznym dopuszczeniem do pracy produkcyjnej w Urzędzie podlega obowiązkowej procedurze testów akceptacyjnych (odbiorowych) w odizolowanym środowisku testowym.

2. Procedura testowa po wdrożeniu musi obejmować weryfikację w trzech obszarach:

- 1) Testy dokładności i poprawności (Niezawodność): Sprawdzenie na próbie testowej (np. 100 historycznych, zanonimizowanych sprawach), czy system AI generuje wyniki postawionych wpisów zgodne z obowiązującymi przepisami prawa i linią orzecniczą;
- 2) Testy odporności na błędy (Cyberbezpieczeństwo): Weryfikacja, jak system reaguje na wprowadzenie danych niekompletnych, błędnych lub próbę manipulacji algorytmem;
- 3) Testy podatności na stronniczość (Bezstronność): Sprawdzenie, czy algorytm nie dyskryminuje osób ze względu na wiek, płeć, miejsce zamieszkania czy status materialny.

3. Pozytywny wynik testów, potwierdzony protokołem odbioru technologicznego AI, jest warunkiem koniecznym do uruchomienia systemu dla mieszkańców lub pracowników.

4. Wprowadza się obowiązek okresowego przeglądu powdrożeniowego. Wyznaczony właściciel systemu (kierownik komórki merytorycznej) we współpracy z Wydziałem Informatyki ma obowiązek:

- 1) Raz na 6 miesięcy (dla systemów niskiego ryzyka) lub raz na kwartał (dla systemów wysokiego ryzyka) dokonać losowej kontroli ludzkiej (audytu) min. 5% spraw przetworzonych przez AI;
- 2) Sporządzić raport z kontroli wykazujący, czy skuteczność i bezstronność systemu nie spadła w czasie eksploatacji (weryfikacja tzw. dryfu modelu);
- 3) W przypadku wykrycia, że system AI generuje błędy, halucynacje prawne lub wykazuje stronniczość, kierownik komórki organizacyjnej ma obowiązek natychmiastowego wyłączenia systemu i zgłoszenia incydentu do dostawcy oprogramowania oraz Inspektora Ochrony Danych.

§ 11. 1. Przed wdrożeniem jakiegokolwiek systemu AI zaliczanego do kategorii wysokiego ryzyka, w szczególności systemów służących do monitorowania, oceny pracy lub zarządzania zasobami ludzkimi, Urząd ma obowiązek poinformowania o tym fakcie zatrudnionych pracowników.

2. Informacja, o której mowa w ust. 1, musi zostać przekazana na co najmniej 14 dni przed planowanym uruchomieniem systemu i zawierać jasny opis przeznaczenia technologii oraz jej wpływu na warunki pracy.

3. Urząd ma obowiązek powiadomić pracowników, którzy będą podlegali działaniu systemu AI lub wchodzili z nim w bezpośrednią interakcję w ramach wykonywanych obowiązków służbowych, o fakcie wdrożenia takiego narzędzia.

§ 12. 1. Przed rozpoczęciem użytkowania systemu AI wysokiego ryzyka, komórka merytoryczna wnioskująca o wdrożenie systemu, we współpracy z Radcą Prawnym oraz Inspektorem Ochrony Danych, ma obowiązek przeprowadzić Ocenę skutków dla praw podstawowych (ang. Fundamental Rights Impact Assessment – FRIA).

2. Ocena FRIA musi przybrać formę pisemnego raportu i zawierać:

- 1) Opis procesów, w których system AI będzie stosowany oraz okres jego planowanego użytkowania;
- 2) Wykaz konkretnych praw podstawowych mieszkańców (np. prawo do równego traktowania, prawo do prywatności, prawo do dobrej administracji), które mogą zostać naruszone lub ograniczone przez działanie algorytmu;
- 3) Szczegółowy plan środków technicznych i organizacyjnych mających na celu zminimalizowanie zidentyfikowanych ryzyk;
- 4) Wyniki oceny FRIA są niezwłocznie przekazywane do właściwego krajowego organu nadzorczego ds. sztucznej inteligencji, zgodnie z obowiązującymi przepisami krajowymi.

§ 13. 1. Każdy materiał graficzny, fotograficzny, audio oraz wideo (w tym animacje) wytworzony przy użyciu systemów sztucznej inteligencji (AI) lub istotnie przez nie zmodyfikowany, przed publikacją w kanałach informacyjnych (strona WWW, Biuletyn Informacji Publicznej, media społecznościowe, materiały drukowane) musi zostać zweryfikowany pod kątem realizmu oraz ryzyka wprowadzenia odbiorcy w błąd.

2. Bezwzględnemu obowiązkowi widocznego oznaczania podlegają wszelkie materiały fotograficzne i wideo, które przedstawiają osoby, obiekty, miejsca lub zdarzenia w sposób fotorealistyczny (spełniający kryteria deep fake w rozumieniu art. 3 pkt 60 Aktu o AI), jeśli przeciętny odbiorca mógłby uznać je za autentyczne dokumenty, prawdziwe zdjęcia lub rzeczywiste nagrania.

3. Prawidłowe i widoczne oznaczenie materiału, o którym mowa w ust. 2, polega na:

- 1) Nałożeniu na grafikę/wideo w sposób trwały i czytelny znaku graficznego lub tekstu: „Materiał wygenerowany przez AI” lub „Materiał zmodyfikowany przy użyciu AI”;
 - 2) Umieszczeniu jednoznacznej informacji w opisie publikacji (np. w treści posta w mediach społecznościowych lub w podpisie pod zdjęciem na stronie WWW).
4. Weryfikacja merytoryczna ani zatwierdzenie materiału foto/wideo przez pracownika Urzędu nie zwalnia z obowiązku umieszczenia widocznego oznaczenia, o którym mowa w ust. 3.

5. Widoczne oznaczenie nie jest wymagane wyłącznie w przypadkach, gdy:

- 1) Materiał ma charakter ewidentnie nierealistyczny, fantastyczny lub abstrakcyjny (np. grafika o charakterze rysunkowym, komiksowym, ikony, schematy), gdzie brak jest ryzyka pomylenia go z rzeczywistością;
- 2) Narzędzia AI zostały użyte wyłącznie do standardowej, technicznej obróbki i edycji istniejącego, autentycznego materiału (np. korekta oświetlenia, usuwanie drobnych szumów, kadrowanie, automatyczny retusz tła), o ile nie zmienia to istotnie kontekstu ani prawdy prezentowanego zdarzenia.

§ 14. 1. Urząd nie może uruchomić produkcyjnie systemu AI wysokiego ryzyka przed dopełnieniem obowiązku jego rejestracji w ogólnodostępnej bazie danych Unii Europejskiej, prowadzonej przez Komisję Europejską.

2. Za prawidłowe i terminowe wprowadzenie danych rejestracyjnych do bazy UE odpowiada Koordynator ds. AI we współpracy z dostawcą systemu AI.

3. W bazie danych, o której mowa w ust. 1, rejestracji podlegają m.in.: nazwa urzędu, dane kontaktowe, nazwa systemu, jego przeznaczenie oraz potwierdzenie przeprowadzenia oceny skutków dla praw podstawowych (FRIA).

§ 15. 1. Wszystkie wdrażane w Urzędzie systemy AI wysokiego ryzyka muszą technicznie umożliwiać automatyczne i ciągłe rejestrowanie zdarzeń (generowanie logów) przez cały okres ich eksploatacji.

2. Rejestry zdarzeń muszą w sposób bezpieczny i niezmienny dokumentować:

- 1) Okresy każdego użycia systemu (datę i godzinę rozpoczęcia oraz zakończenia pracy);
- 2) Dane wejściowe (zapytania) oraz wyniki wygenerowane przez system;
- 3) Tożsamość pracowników Urzędu dokonujących weryfikacji i zatwierdzenia wyników działania algorytmu;
- 4) Zobowiązuje się Wydział Informatyki do zapewnienia środków technicznych gwarantujących przechowywanie logów systemowych przez okres minimum 6 miesięcy od dnia ich utworzenia, w sposób zabezpieczający je przed nieuprawnionym dostępem, modyfikacją lub usunięciem.

Załącznik do
Polityki Bezpiecznego Stosowania Systemów
Sztucznej Inteligencji (AI)

.....
(Miejscowość i data)

Pracownik:

.....
(Imię i nazwisko)

.....
(Stanowisko / wydział)

OŚWIADCZENIE

o zapoznaniu się z Polityką Bezpiecznego Stosowania Systemów Sztucznej Inteligencji (AI)

Niniejszym oświadczam, że zapoznałem/am się z treścią **Polityki Bezpiecznego Stosowania Systemów Sztucznej Inteligencji (AI)** obowiązującej w Urzędzie Miejskim w Suwałkach:

Zobowiązuję się do bezwzględnego przestrzegania zasad określonych w wyżej wymienionym dokumencie, a w szczególności oświadczam, że:

- 1) Nie będę wprowadzać do publicznych i nieautoryzowanych systemów AI jakichkolwiek danych osobowych, informacji poufnych, kodów źródłowych lub innych danych i informacji prawnie chronionych.
- 2) Przyjmuję do wiadomości, że systemy AI stanowią wyłącznie narzędzie pomocnicze, a pełną i osobistą odpowiedzialność za ostateczny rezultat pracy, w tym za weryfikację poprawności merytorycznej i prawnej wygenerowanych treści ponoszę ja jako pracownik urzędu.
- 3) Zobowiązuję się do kontrolowania, czy wyniki działania systemów AI wykorzystywane w moich obowiązkach nie naruszają praw autorskich osób trzecich.
- 4) Zobowiązuję się do natychmiastowego zgłaszania do Wydziału Informatyki wszelkich podejrzeń związanych z wyciekiem danych lub błędnym, niebezpiecznym działaniem systemów AI.

Oświadczam, że treść Polityki AI jest dla mnie całkowicie zrozumiała i zostałem/am poinformowany/a o konsekwencjach służbowych w przypadku naruszenia jej postanowień.

.....
(Czytelny podpis pracownika)