ZARZĄDZENIE NR 140/26
BURMISTRZA DUKLI

z dnia 12 listopada 2026 r.

w sprawie wprowadzenia Regulaminu korzystania z systemów sztucznej inteligencji w Urzędzie Miejskim w Dukli

Na podstawie art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2026 r. poz. 662, z późn. zm.) zarządzam, co następuje:

§ 1. Wprowadza się Regulamin korzystania z systemów sztucznej inteligencji w Urzędzie Miejskim w Dukli, stanowiący załącznik do niniejszego zarządzenia.

§ 2. Regulamin stosuje się do pracowników Urzędu oraz innych osób wykonujących zadania na rzecz Urzędu, jeżeli w związku z wykonywaniem tych zadań korzystają z publicznie dostępnych systemów sztucznej inteligencji, na zasadach określonych w Regulaminie.

§ 3. Kierownicy komórek organizacyjnych są obowiązani zapoznać podległych pracowni z Regulaminem i zapewnić jego przestrzeganie.

§ 4. W sprawach dotyczących ochrony danych osobowych, bezpieczeństwa informacj i bezpieczeństwa systemów teleinformatycznych stosuje się również odrębne regulacje obowiązujące w Urzędzie.

§ 5. Wykonanie zarządzenia powierza się Sekretarzowi Gminy Dukla.

§ 6. Zarządzenie wchodzi w życie z dniem podjęcia.

Burmistrz

Krystyna Andruch

Załącznik do zarządzenia nr 140/26

Burmistrza Dukli

z dnia 12 listopada 2026 r.

REGULAMIN KORZYSTANIA Z SYSTEMÓW SZTUCZNEJ INTELIGENCJI W URZĘDZIE MIEJSKIM W DUKLI

§ 1. Przedmiot i cel Regulaminu

1. Regulamin określa zasady korzystania z publicznie dostępnych narzędzi sztucznej inteligencji, zwanych dalej „narzędziami AI", przez pracowników Urzędu Miejskiego w Dukli.

2. Regulamin dotyczy w szczególności publicznie dostępnych chatbotów i asystentów tekstowych dostępnych w Internecie, takich jak ChatGPT, Gemini, Copilot, Claude lub Perplexity, niezależnie od tego, czy są używane na urządzeniu służbowym czy prywatnym. Wymienione narzędzia stanowią przykłady i nie tworzą zamkniętego katalogu.

3. Celem Regulaminu jest umożliwienie pracownikom korzystania z AI wyłącznie w sposób bezpieczny, zgodny z prawem i niepowodujący ryzyka ujawnienia danych urzędowych, danych osobowych albo informacji chronionych.

4. Korzystanie z narzędzi AI odbywa się z zachowaniem przepisów prawa, w szczególności rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO), rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 (AI Act), ustawy o ochronie informacji niejawnych, ustawy o krajowym systemie cyberbezpieczeństwa oraz Kodeksu pracy.

5. Narzędzia AI mogą być wykorzystywane wyłącznie jako pomoc przy pracach koncepcyjnych, redakcyjnych i językowych, w szczególności do poprawy stylu, przygotowania roboczego szkicu, tłumaczenia ogólnych treści, tworzenia streszczeń, zestawień lub propozycji sformułowań.

§ 2. Zasada ogólna

1. Pracownik może korzystać z publicznie dostępnego narzędzia AI, jeżeli korzystanie z niego nie wiąże się z wprowadzaniem danych osobowych, informacji niepublicznych, informacji chronionych prawem ani innych danych, których ujawnienie mogłoby naruszyć bezpieczeństwo informacji, interes Urzędu lub Gminy.

2. Dopuszczalne jest korzystanie z narzędzi AI na podstawie ogólnych, publicznie dostępnych, fikcyjnych lub całkowicie zanonimizowanych treści, o ile nie zachodzi ryzyko identyfikacji osoby lub powiązania treści z konkretną sprawą.

3. Jeżeli wykonanie zadania wymaga wykorzystania danych urzędowych, danych osobowych albo informacji nieudostępnionych publicznie, korzystanie z publicznie dostępnego narzędzia AI jest zabronione.

4. Brak wyraźnego zakazu w Regulaminie nie oznacza dopuszczenia danego sposobu korzystania z AI. W razie wątpliwości pracownik nie wprowadza danych do narzędzia AI i zasięga opinii przełożonego lub Inspektora Ochrony Danych.

§ 3. Informacje zabronione

1. Zabrania się wprowadzania do publicznie dostępnych narzędzi AI jakichkolwiek informacji urzędowych, w szczególności:

a) danych osobowych, w tym imienia i nazwiska, adresu, numeru PESEL, numeru dokumentu tożsamości, numeru telefonu, adresu e-mail, numeru sprawy, sygnatury, numeru pojazdu, daty urodzenia oraz innych danych umożliwiających identyfikację osoby;

b) danych szczególnych kategorii, o których mowa w art. 9 RODO, w tym danych o zdrowiu, religii, pochodzeniu etnicznym, poglądach politycznych, orientacji seksualnej lub danych biometrycznych;

c) danych dotyczących wyroków skazujących i czynów zabronionych, o których mowa w art. 10 RODO;

d) treści wniosków, pism, decyzji, postanowień, zaświadczeń, umów, protokołów, opinii, projektów dokumentów, korespondencji urzędowej oraz innych materiałów związanych ze sprawami prowadzonymi przez Urząd;

e) informacji niejawnych oraz informacji objętych tajemnicą prawnie chronioną;

f) informacji o postępowaniach, kontrolach, zamówieniach publicznych, negocjacjach, zabezpieczeniach informatycznych, podatnościach, hasłach, loginach, kluczach, tokenach i innych danych uwierzytelniających;

g) informacji dotyczących finansów, majątku, zatrudnienia, organizacji pracy, zamiarów Urzędu albo interesu Gminy, które nie zostały udostępnione publicznie.

h) informacji z wewnętrznych systemów teleinformatycznych Urzędu, w tym z systemów dziedzinowych, jeżeli zawierają dane lub informacje, których wprowadzanie jest zabronione.

2. Zanonimizowanie danych nie może polegać wyłącznie na usunięciu imienia i nazwiska. Należy usunąć lub zastąpić również wszelkie inne dane umożliwiające identyfikację osoby albo powiązanie treści z konkretną sprawą.

3. Jeżeli pracownik chce wykorzystać AI do opracowania tekstu dotyczącego sprawy urzędowej, może wprowadzić wyłącznie ogólny opis problemu, dane fikcyjne albo treść po całkowitym usunięciu danych identyfikujących i informacji niejawnych.

§ 4. Sposób korzystania z narzędzi AI

1. Pracownik korzysta z narzędzi AI wyłącznie w celu wykonania zadania służbowego lub przygotowania materiału pomocniczego.

2. Zabrania się wykorzystywania AI do podejmowania decyzji, ustalania rozstrzygnięć, kwalifikowania prawnego stanów faktycznych albo zastępowania samodzielnej oceny pracownika.

3. Zabrania się obchodzenia zabezpieczeń informatycznych Urzędu, polityk bezpieczeństwa, blokad sieciowych albo ograniczeń dostępu do stron internetowych.

4. Zabrania się wykorzystywania AI do tworzenia, modyfikowania lub uruchamiania kodu, skryptów, reguł sieciowych, konfiguracji systemów informatycznych albo działań mogących wpłynąć na bezpieczeństwo systemów Urzędu, chyba że pracownik posiada odrębne upoważnienie.

5. Pracownik nie może logować się do narzędzi AI przy użyciu służbowego adresu e-mail, hasła służbowego, konta urzędowego albo danych uwierzytelniających wykorzystywanych w systemach Urzędu.

6. Pracownik nie może udostępniać w narzędziach AI linków do wewnętrznych systemów Urzędu, dokumentów z akt spraw ani plików zawierających dane urzędowe.

§ 5. Weryfikacja wyników działania AI

1. Treść wygenerowana przez narzędzie AI stanowi materiał pomocniczy i nie może być traktowana jako samodzielne, wiarygodne źródło informacji, opinia prawna ani treść urzędowa. Nie może być uznana za prawdziwą, kompletną ani aktualną wyłącznie dlatego, że została wygenerowana automatycznie.

2. Przed wykorzystaniem wyniku AI pracownik jest obowiązany zweryfikować go pod względem zgodności ze stanem faktycznym, aktualności, zgodności z obowiązującymi przepisami, poprawności przywołanych podstaw prawnych, orzeczeń, danych, dat, nazw, kwot i źródeł, a także kompletności i logicznej spójności.

3. W szczególności pracownik jest obowiązany samodzielnie sprawdzić każdą przywołaną podstawę prawną, orzeczenie, publikację lub cytat. Narzędzia AI mogą generować treści nieprawdziwe, nieaktualne albo nieistniejące.

4. Treść wygenerowana przez AI może zostać wykorzystana w dokumencie urzędowym wyłącznie po jej zweryfikowaniu, uzupełnieniu i zaakceptowaniu przez pracownika odpowiedzialnego za przygotowanie, zatwierdzenie lub podpisanie dokumentu.

5. Za treść dokumentu urzędowego odpowiada pracownik, który go przygotowuje, zatwierdza lub podpisuje, zgodnie z przyznanymi mu uprawnieniami i zakresem obowiązków.

6. Zabrania się wykorzystywania niezweryfikowanego wyniku AI jako podstawy decyzji administracyjnej, postanowienia, zaświadczenia, odpowiedzi na wniosek, opinii prawnej, stanowiska Urzędu albo innego działania wywołującego skutki prawne.

§ 6. Ochrona danych osobowych i bezpieczeństwo informacji

1. Korzystanie z publicznie dostępnych narzędzi AI nie może powodować przetwarzania danych osobowych w sposób niezgodny z RODO.

2. Jeżeli wykonanie zadania jest możliwe bez danych osobowych, pracownik stosuje dane ogólne, zagregowane, fikcyjne lub całkowicie zanonimizowane.

3. W razie przypadkowego wprowadzenia danych osobowych do narzędzia AI pracownik jest obowiązany niezwłocznie zgłosić ten fakt zgodnie z § 8 Regulaminu.

4. Pracownik jest obowiązany stosować zasady bezpieczeństwa informacji obowiązujące w Urzędzie. Wykorzystywanie urządzeń prywatnych oraz sieci publicznych do zadań służbowych podlega ograniczeniom wynikającym z odrębnych regulacji bezpieczeństwa informacji obowiązujących w Urzędzie.

5. Zabrania się zapisywania w historii rozmów, udostępniania osobom trzecim albo wykorzystywania w innych celach treści wygenerowanych przez AI, jeżeli zawierają one jakiekolwiek informacje dotyczące Urzędu lub osób trzecich.

§ 7. Prawa autorskie i prawa osób trzecich

1. Pracownik korzystający z narzędzia AI jest obowiązany przestrzegać przepisów o prawie autorskim, prawach pokrewnych, ochronie wizerunku, danych osobowych, tajemnicy przedsiębiorstwa oraz innych praw osób trzecich.

2. Przed wykorzystaniem materiału wygenerowanego przez AI w oficjalnej działalności Urzędu pracownik weryfikuje, czy jego wykorzystanie nie narusza praw osób trzecich.

3. Zabrania się wprowadzania do narzędzi AI utworów, baz danych, materiałów objętych tajemnicą przedsiębiorstwa albo innych chronionych treści w zakresie wykraczającym poza dozwolony użytek lub uprawnienia Urzędu.

§ 8. Zgłaszanie incydentów

1. Pracownik jest obowiązany niezwłocznie, nie później niż w dniu stwierdzenia zdarzenia (a w przypadku zdarzeń poza godzinami pracy – niezwłocznie po rozpoczęciu pracy w najbliższym dniu roboczym), zgłosić:

a) bezpośredniemu przełożonemu;

b) Inspektorowi Ochrony Danych – w przypadku zdarzeń dotyczących danych osobowych;

2. przypadkowe wprowadzenie do narzędzia AI danych osobowych, danych urzędowych, informacji niejawnych albo innych informacji, których wprowadzanie było zabronione;

3. podejrzenie ujawnienia informacji osobie nieuprawnionej;

4. naruszenie lub podejrzenie naruszenia bezpieczeństwa konta, urządzenia albo systemu informatycznego Urzędu;

5. wykrycie w treści wygenerowanej przez AI danych osobowych, danych wrażliwych, informacji niejawnych albo innych informacji, których obecność w narzędziu jest niedopuszczalna;

6. inne zdarzenie mogące skutkować naruszeniem bezpieczeństwa informacji lub ochrony danych osobowych.

7. W przypadku podejrzenia naruszenia ochrony danych osobowych stosuje się procedurę postępowania w przypadku naruszenia ochrony danych osobowych obowiązującą w Urzędzie.

8. Pracownik nie usuwa samodzielnie dokumentacji, logów ani innych materiałów mogących służyć wyjaśnieniu zdarzenia, jeżeli został o tym poinformowany przez osobę prowadzącą postępowanie wyjaśniające.

§ 9. Kompetencje pracowników

1. Pracownik może korzystać z narzędzi AI wyłącznie po zapoznaniu się z Regulaminem oraz zasadami bezpieczeństwa obowiązującymi w Urzędzie.

2. Urząd zapewnia, stosownie do potrzeb, szkolenia lub materiały informacyjne dotyczące bezpiecznego i odpowiedzialnego korzystania z AI.

3. Pracownik jest obowiązany kierować się zasadą ostrożności, a w przypadku braku pewności co do dopuszczalności wprowadzenia danych — powstrzymać się od ich wprowadzenia.

§ 10. Odpowiedzialność

1. Korzystanie z narzędzi AI nie ogranicza odpowiedzialności pracownika wynikającej z przepisów prawa, zakresu obowiązków, upoważnienia albo powierzonego zadania.

2. Naruszenie Regulaminu stanowi naruszenie obowiązków pracowniczych i może skutkować odpowiedzialnością porządkową przewidzianą w Kodeksie pracy, w szczególności upomnieniem lub naganą.

3. W przypadku ciężkiego naruszenia podstawowych obowiązków pracowniczych pracodawca może stosować środki przewidziane w Kodeksie pracy, w tym rozwiązanie umowy o pracę bez wypowiedzenia, jeżeli występują przesłanki określone w art. 52 Kodeksu pracy.

4. Naruszenie Regulaminu może również skutkować odpowiedzialnością cywilną, dyscyplinarną albo karną, jeżeli zachodzą przesłanki przewidziane odrębnymi przepisami.

5. Regulamin nie ustanawia kar pieniężnych ani innych sankcji niewynikających wprost z przepisów powszechnie obowiązującego prawa.

§ 11. Postanowienia końcowe

1. W przypadku rozbieżności między Regulaminem a przepisami powszechnie obowiązującego prawa pierwszeństwo mają przepisy prawa.

2. Regulamin podlega przeglądowi nie rzadziej niż raz w roku oraz każdorazowo w przypadku istotnej zmiany przepisów dotyczących sztucznej inteligencji, ochrony danych osobowych, cyberbezpieczeństwa albo organizacji pracy Urzędu.

3. Jeżeli Urząd zapewni pracownikom licencjonowane narzędzie AI działające w kontrolowanym środowisku informatycznym, zasady jego korzystania zostaną określone w odrębnym zarządzeniu.

4. Regulamin wchodzi w życie z dniem podjęcia.