

ZARZĄDZENIE NR 85/2026
WÓJTA GMINY GŁÓWCZYCE
z dnia 2 lipca 2026 r.

**w sprawie wprowadzenia Instrukcja bezpiecznego korzystania z narzędzi
sztucznej inteligencji (AI) w Urzędzie Gminy Główny**

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2026 r. poz. 662)

zarządzam, co następuje:

§ 1. Wprowadzam do stosowania Instrukcję bezpiecznego korzystania z narzędzi sztucznej inteligencji (AI) w Urzędzie Gminy Główny – wymagania RODO.

§ 2. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
Rafał Teterka

Instrukcja bezpiecznego korzystania z narzędzi sztucznej inteligencji (AI) w Urzędzie – wymagania RODO

Spis treści

1. Cel instrukcji	2
2. Zasada podstawowa.....	2
3. Dane, których nie wolno udostępniać do AI.....	2
3.1. Dane osobowe.....	2
3.2. Szczególne kategorie danych osobowych	3
3.3. Dane pracowników.....	3
3.4. Dane mieszkańców i klientów Urzędu.....	4
3.5. Dane finansowe.....	4
3.6. Informacje poufne Urzędu	5
4. Jak przygotować dokument do wykorzystania w AI.....	5
5. Dopuszczalne zastosowania AI	6
6. Czego AI nie powinna robić	6
7. Obowiązki pracownika	7
8. Postępowanie w przypadku naruszenia	7
9. Odpowiedzialność	8
Załącznik – szybka checklista	8

1. Cel instrukcji

Celem niniejszej instrukcji jest określenie zasad bezpiecznego korzystania przez pracowników Urzędu z narzędzi opartych na sztucznej inteligencji (AI), w szczególności generatywnych modeli językowych, w sposób zgodny z przepisami RODO, ustawą o ochronie danych osobowych, zasadami bezpieczeństwa informacji oraz obowiązującymi procedurami wewnętrznymi.

Instrukcja ma na celu ograniczenie ryzyka nieuprawnionego ujawnienia danych osobowych, informacji prawnie chronionych oraz informacji stanowiących tajemnicę Urzędu.

2. Zasada podstawowa

Do ogólnodostępnych narzędzi AI nie wolno wprowadzać żadnych informacji, które umożliwiają identyfikację osoby fizycznej lub zawierają informacje poufne, chyba że narzędzie zostało oficjalnie dopuszczone do przetwarzania takich danych przez Urząd.

Pracownik powinien zawsze przyjąć zasadę:

Jeżeli dokumentu nie można opublikować w Internecie – nie należy go wprowadzać do publicznego narzędzia AI.

3. Dane, których nie wolno udostępniać do AI

3.1. Dane osobowe

Zakazane jest wpisywanie:

- imion i nazwisk,
- numerów PESEL,
- numerów dowodów osobistych,
- numerów paszportów,
- numerów prawa jazdy,
- adresów zamieszkania,
- adresów e-mail osób fizycznych,
- numerów telefonów,
- dat urodzenia,
- podpisów,

- numerów rachunków bankowych,
 - numerów identyfikacyjnych pracowników,
 - numerów akt spraw,
 - sygnatur umożliwiających identyfikację osoby.
-

3.2. Szczególne kategorie danych osobowych

Bezwzględnie zabrania się udostępniania danych dotyczących:

- stanu zdrowia,
 - niepełnosprawności,
 - danych biometrycznych,
 - danych genetycznych,
 - poglądów politycznych,
 - przekonań religijnych,
 - przynależności związkowej,
 - orientacji seksualnej,
 - danych dotyczących wyroków skazujących,
 - danych dotyczących postępowań administracyjnych lub dyscyplinarnych.
-

3.3. Dane pracowników

Nie wolno przekazywać:

- akt osobowych,
- ocen okresowych,
- informacji o wynagrodzeniach,
- informacji kadrowych,
- informacji o absencjach,
- danych z rekrutacji,
- CV kandydatów,
- dokumentacji medycznej pracowników,
- numerów identyfikacyjnych.

3.4. Dane mieszkańców i klientów Urzędu

Zakazane jest wprowadzanie:

- wniosków mieszkańców,
- podań,
- skarg,
- petycji,
- decyzji administracyjnych zawierających dane osobowe,
- dokumentacji świadczeń,
- danych podatników,
- danych dotyczących pomocy społecznej,
- danych dzieci,
- danych rodzin.

3.5. Dane finansowe

Nie wolno udostępniać:

- informacji o rachunkach bankowych,
- numerów faktur zawierających dane osób,
- dokumentów księgowych,
- danych płacowych,
- informacji podatkowych,
- deklaracji podatkowych.

3.6. Informacje poufne Urzędu

Zakazane jest udostępnianie:

- projektów uchwał przed publikacją,
- projektów decyzji,
- projektów zarządzeń,
- wewnętrznych analiz,
- audytów,
- wyników kontroli,
- dokumentów strategicznych,
- planów inwestycyjnych,
- danych dotyczących cyberbezpieczeństwa,
- informacji o infrastrukturze IT,
- haseł,
- kluczy dostępowych,
- konfiguracji systemów,
- kopii baz danych.

4. Jak przygotować dokument do wykorzystania w AI

Przed wprowadzeniem dokumentu do AI należy:

1. usunąć wszystkie dane osobowe,
2. zastąpić imiona i nazwiska oznaczeniami (np. Pracownik A, Mieszkaniec 1),
3. usunąć numery PESEL,
4. usunąć adresy,
5. usunąć numery telefonów,
6. usunąć adresy e-mail,
7. usunąć numery spraw,
8. usunąć numery decyzji,
9. usunąć podpisy,

10. usunąć wszystkie informacje pozwalające zidentyfikować konkretną osobę.

Przykład:

NIE:

"Jan Kowalski, PESEL 70010112345 złożył wniosek o..."

TAK:

"Mieszkaniec złożył wniosek o..."

5. Dopuszczalne zastosowania AI

Po anonimizacji danych AI może być wykorzystywana m.in. do:

- redagowania pism,
 - poprawy stylistyki dokumentów,
 - tworzenia projektów procedur,
 - opracowywania regulaminów,
 - przygotowywania prezentacji,
 - tworzenia checklist,
 - przygotowywania materiałów szkoleniowych,
 - streszczania aktów prawnych,
 - wyszukiwania podstaw prawnych,
 - przygotowywania wzorów dokumentów,
 - tłumaczeń,
 - tworzenia harmonogramów.
-

6. Czego AI nie powinna robić

AI nie może samodzielnie:

- podejmować decyzji administracyjnych,
- wydawać decyzji wobec obywateli,
- zastępować analizy prawnej wykonywanej przez pracownika,
- podpisywać dokumentów,

- zastępować pracownika w ocenie indywidualnej sprawy,
- decydować o prawach lub obowiązkach obywateli.

Każdy wynik wygenerowany przez AI wymaga weryfikacji przez pracownika.

7. Obowiązki pracownika

Pracownik korzystający z AI jest zobowiązany do:

- zachowania poufności informacji,
 - przestrzegania zasad RODO,
 - stosowania zasady minimalizacji danych,
 - sprawdzania poprawności odpowiedzi AI,
 - niewprowadzania danych osobowych do publicznych narzędzi AI,
 - zgłaszania incydentów związanych z AI do przełożonego lub Inspektora Ochrony Danych.
-

8. Postępowanie w przypadku naruszenia

Jeżeli do narzędzia AI zostały przypadkowo przekazane dane osobowe lub informacje poufne, pracownik powinien niezwłocznie:

1. poinformować przełożonego,
2. zgłosić zdarzenie Inspektorowi Ochrony Danych,
3. opisać zakres ujawnionych informacji,
4. wskazać użyte narzędzie AI,
5. zastosować się do dalszych zaleceń dotyczących obsługi incydentu.

9. Odpowiedzialność

Każdy pracownik korzystający z AI odpowiada za zgodność sposobu wykorzystania narzędzi z:

- RODO,
- ustawą o ochronie danych osobowych,
- przepisami dotyczącymi bezpieczeństwa informacji,
- wewnętrznymi procedurami Urzędu.

Naruszenie zasad określonych w niniejszej instrukcji może skutkować odpowiedzialnością służbową oraz innymi konsekwencjami przewidzianymi przepisami prawa i regulacjami wewnętrznymi.

Załącznik – szybka checklista

Przed użyciem AI odpowiedz na pytania:

- ☐ Czy dokument zawiera dane osobowe?
- ☐ Czy zawiera dane wrażliwe?
- ☐ Czy zawiera dane mieszkańców?
- ☐ Czy zawiera dane pracowników?
- ☐ Czy zawiera informacje poufne?
- ☐ Czy dokument został zanonimizowany?
- ☐ Czy wynik AI zostanie zweryfikowany przez pracownika?
- ☐ Jeżeli na którekolwiek z pierwszych pięciu pytań odpowiedź brzmi „TAK”,
dokument nie powinien zostać przekazany do publicznego narzędzia AI bez
uprzedniej skutecznej anonimizacji lub odpowiednich zabezpieczeń
organizacyjnych i prawnych.