

**w sprawie korzystania z narzędzi sztucznej inteligencji (AI)
w Urzędzie Gminy Malczyce**

Na podstawie art. 30 ust. ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2024 r. poz. 1465 z późn. zm.), w związku z art. 5, 24 i 25 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO) (DZ.URZ.UE 4.5.2016), zarządzam, co następuje:

§ 1. Niniejsze zarządzenie określa zasady korzystania z narzędzi sztucznej inteligencji (AI) przez pracowników Urzędu Gminy Malczyce, w szczególności generatywnych systemów AI, w celu zapewnienia zgodności z przepisami prawa, ochrony danych osobowych, praw autorskich oraz bezpieczeństwa informacji.

§ 2. Definicje:

1. **Sztuczna inteligencja (AI)** – system zdolny do analizowania danych i podejmowania działań w sposób częściowo autonomiczny.
2. **Generatywna AI** – typ AI zdolny do tworzenia nowych treści (tekstów, obrazów, dźwięków, filmów, kodu) często w formie symulowanej komunikacji z człowiekiem.
3. **Narzędzia AI** – ogólnodostępne aplikacje, platformy i systemy wykorzystujące AI, dostępne online lub lokalnie.
4. **Treści stworzone z udziałem AI** – materiały, które powstały w całości lub w znacznej części przy wsparciu narzędzi AI.
5. **Halucynacja AI** – zjawisko polegające na tym, że narzędzie sztucznej inteligencji generuje treści nieprawdziwe lub wprowadzające w błąd, mimo że są one przedstawiane w sposób pozornie logiczny i przekonujący. Halucynacje mogą obejmować m.in. fikcyjne przepisy prawa, nieistniejące orzeczenia sądów, fałszywe dane, zmyślone źródła informacji lub błędne wnioski. Zjawisko to wynika z probabilistycznego działania modeli językowych AI, które tworzą odpowiedzi na podstawie wzorców językowych, a nie wiedzy rzeczywistej.
6. **Weryfikacja merytoryczna** – sprawdzenie treści wygenerowanej przez AI pod względem zgodności z obowiązującym prawem, stanem faktycznym, wewnętrznymi procedurami urzędu oraz poprawnością językową, przez osobę kompetentną w danym zakresie.

7. **DPIA (ocena skutków dla ochrony danych)** – analiza ryzyka dla praw i wolności osób fizycznych, przeprowadzana zgodnie z art. 35 RODO, przed rozpoczęciem przetwarzania danych osobowych przy użyciu narzędzi lub technologii mogących powodować wysokie ryzyko.
8. **Prompt** – polecenie, zapytanie lub zestaw instrukcji wprowadzonych przez użytkownika do narzędzia sztucznej inteligencji, które służy jako podstawa do wygenerowania przez AI odpowiedzi lub innej treści.

§ 3. Obowiązki pracowników

Przed użyciem narzędzia AI pracownik zobowiązany jest:

1. Sprawdzić, czy narzędzie znajduje się na liście zatwierdzonych rozwiązań (wykaz dostępny u Administratora Systemu).
2. Upewnić się, że treści generowane przez AI nie zawierają plagiatów ani nie naruszają praw autorskich.
3. Zweryfikować treści pod kątem zgodności z prawem i stanem faktycznym – AI nie może być jedynym źródłem informacji.
4. W razie wątpliwości co do legalności lub bezpieczeństwa narzędzia – skonsultować się z:
 - Inspektorem Ochrony Danych (RODO),
 - Działem Prawnym (licencje, prawa autorskie),
 - Administratorem Systemów Informatycznych (bezpieczeństwo systemów).

§ 4. Ochrona danych osobowych (RODO)

1. Zabronione jest przetwarzanie w narzędziach AI danych osobowych, chyba że **łącznie spełnione są wszystkie poniższe warunki**:
 - operator narzędzia AI podpisał z Urzędem [nazwa urzędu] umowę powierzenia przetwarzania danych zgodnie z art. 28 RODO,
 - narzędzie zapewnia odpowiednie środki techniczne i organizacyjne, w szczególności:
 - szyfrowanie danych,
 - hosting w UE lub EOG,
 - jasna polityka retencji danych (brak trwałego przechowywania danych bez uzasadnienia),
 - została przeprowadzona **ocena skutków dla ochrony danych (DPIA)**,

- istnieje **ważna podstawa prawna przetwarzania danych osobowych** (np. zgoda, wykonanie obowiązku prawnego, umowy).
- 2. Przed użyciem narzędzia AI do jakiegokolwiek operacji na danych osobowych pracownik musi:
 - upewnić się, że narzędzie znajduje się w wykazie zatwierdzonych rozwiązań z podpisaną umową powierzenia przetwarzania danych,
 - ograniczyć zakres danych do niezbędnego minimum zgodnie z zasadą **minimalizacji danych**.
- 3. W przypadku podejrzenia lub stwierdzenia naruszenia ochrony danych (np. wyciek danych do nieautoryzowanego narzędzia AI), pracownik zobowiązany jest:
 - **niezwłocznie powiadomić Inspektora Ochrony Danych**,
 - podjąć działania zgodnie z obowiązującą w urzędzie procedurą reagowania na incydenty.

§ 5. Prawa autorskie i odpowiedzialność

1. Treści tworzone z udziałem AI mogą podlegać ochronie prawnej – pracownik musi:
 - znać zasady licencyjne i warunki korzystania z danego narzędzia,
 - nie kopiować treści chronionych bez odpowiedniego zezwolenia.
2. Odpowiedzialność za treści stworzone z pomocą AI spoczywa na pracowniku i jego przełożonym.

§ 6. Dezinformacja i weryfikacja źródeł

1. Narzędzia AI mogą generować:
 - nieprawdziwe informacje o faktach, osobach i instytucjach,
 - fałszywe odniesienia do przepisów prawa lub orzeczeń (tzw. halucynacje AI).
2. Pracownik ma obowiązek weryfikować treści z AI przed ich wykorzystaniem.
3. Zabrania się powielania niesprawdzonych informacji z AI w dokumentach urzędowych lub komunikacji z obywatelami.

§ 7. Ograniczenia w stosowaniu narzędzi AI w zadaniach merytorycznych

1. Narzędzia sztucznej inteligencji nie mogą być wykorzystywane jako **jedyny środek** przygotowania treści w sprawach wymagających analizy prawnej, indywidualnego rozstrzygnięcia lub wykładni przepisów. Dotyczy to w szczególności:
 1. odpowiedzi na wnioski o udostępnienie informacji publicznej,
 2. czynności podejmowanych w ramach postępowań administracyjnych,

3. decyzji, postanowień, wezwań i innych pism wywołujących skutki prawne,
 4. dokumentów dotyczących zamówień publicznych (SIWZ, SWZ, umowy, ogłoszenia),
 5. treści publikowanych w ramach oficjalnych kanałów komunikacji z obywatelami (strony internetowe, media społecznościowe, biuletyny),
 6. materiałów o charakterze promocyjnym lub informacyjnym, których forma i treść mają wpływ na postrzeganie organu publicznego lub kształtowanie opinii społecznej.
2. Narzędzia AI mogą być wykorzystywane **pomocniczo**, np. w celu:
- przygotowania wstępnych szkiców,
 - tworzenia struktury dokumentu,
 - sprawdzania poprawności językowej,
 - streszczania treści lub porządkowania danych.
3. Ostateczna treść dokumentu musi być każdorazowo:
- **zweryfikowana przez pracownika merytorycznego,**
 - **zgodna z przepisami prawa,**
 - **zatwierdzona przez osobę odpowiedzialną za daną sprawę.**
4. Niedopuszczalne jest uzasadnianie decyzji administracyjnych, ocen prawnych lub stanowisk urzędu wyłącznie na podstawie wyników wygenerowanych przez narzędzia AI.

§ 8. Postanowienia końcowe

1. Nadzór nad stosowaniem niniejszego zarządzenia sprawuje Inspektor Ochrony Danych oraz Administrator Systemu.
2. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Malczyce

Piotr Frankowski

