

Zarządzenie nr 12/2025/26 Rektora
Wyższej Szkoły Zarządzania Ochroną Pracy w Katowicach
z dnia 21 września 2026 r.
w sprawie zasad wykorzystania narzędzi AI w ramach czynności służbowych

Na podstawie ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (tj. Dz. U. z 2024 r. poz. 1571 z późn. zm.) oraz w celu zapewnienia zgodności z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. ustalającym zharmonizowane przepisy dotyczące sztucznej inteligencji (AI Act), Polityki Bezpieczeństwa Informacji WSZOP zarządza się, co następuje:

Cel i zakres stosowania

§ 1

1. Zarządzenie określa zasady wykorzystania narzędzi sztucznej inteligencji, w tym dużych generatywnych modeli językowych przez pracowników WSZOP w ramach czynności służbowych.
2. Zarządzenie ma na celu:
 - 1) ochronę danych osobowych, informacji poufnych, w tym własności intelektualnej Uczelni
 - 2) zapewnienie zgodności z RODO, AI Act oraz Polityką Bezpieczeństwa informacji WSZOP
 - 3) minimalizację ryzyka prawnego, reputacyjnego Uczelni związanego z użyciem AI
 - 4) promowanie odpowiedzialnego i etycznego wykorzystania AI w procesach uczelnianych.

Definicje

§ 2

1. **LLM (Large Language Model)** – duży model językowy oparty na architekturze transformera, służący do rozumienia i generowania języka naturalnego; może stanowić podstawę systemów multimodalnych przetwarzających również obrazy, audio i wideo (np. modele GPT – OpenAI, Gemini – Google, Claude – Anthropic, Grok – xAI).
2. **Narzędzie AI** – aplikacja, usługa lub platforma wykorzystująca jeden lub więcej modeli AI (w tym LLM, modele dyfuzyjne, modele wideo), np. ChatGPT, Gemini, Grok, Claude, DALL-E 3, Sora, Manus.
3. **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej
4. **Informacje poufne** – wszelkie informacje, które nie zostały przeznaczone do publicznego udostępnienia albo których ujawnienie, wykorzystanie lub utrata kontroli nad nimi mogłyby naruszyć interes Uczelni, prawa osób trzecich, bezpieczeństwo informacji lub obowiązek poufności (dane, materiały, dokumenty lub ich fragmenty, niezależnie od formy, dotyczące Uczelni, pracowników, studentów, kandydatów, absolwentów, partnerów, kontrahentów, projektów lub działalności Uczelni)
5. **Prompt** – krótka instrukcja, polecenie lub pytanie wpisane przez użytkownika, które ma wykonać model AI – np. odpowiedzieć, wygenerować tekst, przeanalizować dane.

Zakres dozwolonego użycia narzędzi AI

§ 3

1. Korzystanie z narzędzi AI, w tym dużych modeli językowych (LLM) i czatów AI, w działalności dydaktycznej, naukowej, administracyjnej i organizacyjnej Uczelni jest dopuszczalne, pod warunkiem że nie wiąże się z przekazywaniem danych osobowych ani informacji poufnych, z zastrzeżeniem § 5 pkt 3.

2. Zakaz przekazywania do narzędzi AI treści zawierających dane osobowe lub informacje poufne wynika z ryzyka ich transmisji i przetwarzania na serwerach operatorów narzędzi AI oraz braku kontroli nad zakresem, okresem i celem dalszego przetwarzania przekazanych treści.

§ 4

1. Niedopuszczalne jest w szczególności wprowadzanie, przesyłanie, kopiowanie następujących informacji:
 - 1) danych osobowych, w tym imion i nazwisk, adresów, numerów telefonów, adresów e-mail, numerów PESEL, numerów dokumentów tożsamości, danych kadrowych, danych płacowych i danych kontaktowych
 - 2) szczególnych kategorii danych osobowych, w tym danych dotyczących zdrowia, niepełnosprawności, danych biometrycznych, przekonań religijnych lub światopoglądowych, przynależności związkowej, pochodzenia rasowego lub etnicznego, orientacji seksualnej lub życia seksualnego
 - 3) danych dotyczących postępowań dyscyplinarnych, skarg, sporów, wypadków, spraw socjalnych, ocen okresowych, rekrutacji, stypendiów, pomocy materialnej, egzaminów, zaliczeń
 - 4) dokumentów zawierających dane osobowe lub informacje chronione Uczelni, w szczególności pism, umów, aneksów, faktur, opinii prawnych, protokołów, uchwał, zarządzeń nieprzeznaczonych do publikacji, korespondencji, akt osobowych, podań, ocen, raportów i wniosków, projektów
 - 5) informacji objętych tajemnicą przedsiębiorstwa, tajemnicą zawodową, tajemnicą wynikającą z umowy albo obowiązkiem zachowania poufności
 - 6) wyników badań przed ich upublicznieniem, danych badawczych, danych z projektów, opisów rozwiązań technicznych, kodu źródłowego, dokumentacji systemów, konfiguracji bezpieczeństwa, haseł, kluczy dostępowych, tokenów i danych uwierzytelniających
 - 7) nieprzeznaczonych do publikacji informacji dotyczących strategii, planów rozwoju, planów finansowych, negocjacji, ofert, zamówień, postępowań zakupowych, projektów inwestycyjnych, współpracy z partnerami, audytów i analiz wewnętrznych
 - 8) materiałów przekazanych Uczelni przez osoby trzecie, jeżeli ich wykorzystanie w narzędziu AI nie zostało wyraźnie dopuszczone przez uprawniony podmiot.
2. Zakaz, o którym mowa w ust. 3, obejmuje wszelkie formy danych i informacji, w szczególności wpisanie tekstu, załączenie pliku tekstowego, obrazu, skanu, fotografii, nagrania dźwiękowego i nagrania wideo.
3. Zakaz ma zastosowanie także wtedy, gdy dane lub dokumenty są przesyłane do AI w celu korekty, streszczenia, tłumaczenia, transkrypcji, analizy, klasyfikacji, oceny, generowania odpowiedzi lub przygotowania projektu dokumentu.

§ 5

Dopuszcza się wykorzystywanie narzędzi AI do zadań niewymagających ujawnienia danych osobowych, informacji chronionych Uczelni ani treści chronionych, w szczególności do:

- 1) opracowywania ogólnych konspektów, propozycji struktury dokumentów i list kontrolnych
- 2) korekty stylistycznej lub językowej tekstów uprzednio pozbawionych danych chronionych
- 3) modyfikacji zdjęć, w tym zawierających dane osobowe (wizerunek) przeznaczonych do publikacji na stronie Uczelni
- 4) tłumaczenia zanonimizowanych treści
- 5) przygotowywania propozycji materiałów dydaktycznych, ćwiczeń, pytań kontrolnych lub przykładów o charakterze ogólnym
- 6) wyjaśniania pojęć, tworzenia przykładów, syntez i zestawień na podstawie informacji publicznie dostępnych
- 7) wsparcia technicznego, programistycznego lub redakcyjnego, pod warunkiem że prompt, załączniki i wynik nie zawierają informacji chronionych.

Obowiązki użytkownika

§ 6

1. Przed wprowadzeniem treści do narzędzia AI użytkownik jest obowiązany ocenić, czy treść nie zawiera:
 - 1) danych osobowych
 - 2) informacji poufnych
 - 3) treści chronionych prawem autorskim lub prawami pokrewnymi w sposób wykluczający ich wykorzystanie przez systemy AI.
2. W razie stwierdzenia, że treść obejmuje którykolwiek z elementów wymienionych, w ust. 1 jej przekazanie do narzędzia AI jest niedozwolone.
3. W razie wątpliwości użytkownik odstępuje od wprowadzenia danych do narzędzia AI i zwraca się o opinię do Inspektora Ochrony Danych.
4. Użytkownik niezwłocznie zgłasza Inspektorowi Ochrony Danych:
 - 1) przypadkowe wprowadzenie danych osobowych lub poufnych do narzędzia AI
 - 2) podejrzenie wycieku danych lub naruszenia bezpieczeństwa
5. W przypadku generowania treści (tekst, obraz, wideo, dźwięk) przy użyciu AI użytkownik jest obowiązany oznaczyć treść informacją: *Treść wygenerowana przy użyciu AI: (nazwa narzędzia)* – zgodnie z art. 50 AI Act.

Postanowienia końcowe

§ 7

1. Naruszenie postanowień Zarządzenia stanowi ciężkie naruszenie obowiązków pracowniczych.
2. W przypadku wycieku danych osobowych Uczelnia jest obowiązana zgłosić naruszenie do Prezesa Urzędu Ochrony Danych Osobowych (UODO) w ciągu 72 godzin (art. 33 RODO).
3. Zarządzenie wchodzi w życie z dniem 1 października 2026 r.

REKTOR

prof. dr hab. inż. Bohdan Mochnacki