Załącznik do Zarządzenia Rektora WAT
nr 21/RKR/2025 z dnia 3 lipca 2025 r.

Regulamin stosowania rozwiązań sztucznej inteligencji w Wojskowej Akademii Technicznej

Rozdział I – Postanowienia ogólne

§1
Cel regulaminu

1. Regulamin określa zasady wdrażania, stosowania i monitorowania rozwiązań sztucznej inteligencji (dalej: AI) w działalności naukowej, dydaktycznej oraz administracyjnej Wojskowej Akademii Technicznej (dalej: WAT).
2. Celem regulaminu jest zapewnienie zgodności rozwoju i zastosowania AI z wartościami etycznymi, przepisami prawa, zasadami bezpieczeństwa narodowego oraz misją WAT.
3. Wydział może uchwalić szczegółowe zasady korzystania z narzędzi AI, które będą zgodne z niniejszym regulaminem.

§2
Zakres stosowania

Regulamin obowiązuje wszystkich pracowników, współpracowników oraz studentów realizujących zadania w WAT lub na rzecz WAT z wykorzystaniem narzędzi i systemów AI.

§3
Definicje

Na potrzeby niniejszego regulaminu przyjmuje się następujące definicje:
1. AI (sztuczna inteligencja) – metody i technologie informatyczne zdolne do wykonywania zadań wymagających inteligencji ludzkiej, takich jak uczenie maszynowe, przetwarzanie języka naturalnego, generowanie tekstu i obrazu, rozpoznawanie obrazów, analiza predykcyjna itp.;
2. System AI – system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który - na potrzeby wyraźnych lub dorozumianych celów - wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne;
3. System AI wysokiego ryzyka – system AI, którego niewłaściwe działanie może prowadzić do naruszenia praw człowieka, bezpieczeństwa lub interesu publicznego;
4. Użytkownik AI – każda osoba fizyczna lub jednostka organizacyjna korzystająca z rozwiązań AI w WAT;
5. Pracownik – nauczyciel akademicki, jak i pracownik niebędący nauczycielem akademickim zatrudniony w WAT na podstawie stosunku pracy oraz żołnierz zawodowy pełniący służbę w WAT;
6. Student – doktorant, student, uczestnik studiów podyplomowych, kursów kwalifikacyjnych i doskonalących oraz innych form kształcenia;

7. Współpracownik – osoba współpracująca z WAT na podstawie umowy cywilnoprawnej (umowa o dzieło, umowa zlecenie, umowa z dostawcą);
8. Wydział – jednostka organizacyjna realizująca, w ramach jednej lub kilku dyscyplin naukowych, zadania określone w § 39 ust. 1 oraz § 40 ust. 4 Statutu WAT.

Rozdział II – Zasady ogólne stosowania AI

§4
Zgodność z przepisami i normami

Wszystkie systemy AI stosowane w WAT muszą być zgodne z obowiązującym prawem, w tym z:

a) Rozporządzeniem UE w sprawie sztucznej inteligencji (AI Act)[1];
b) przepisami dotyczącymi ochrony danych osobowych w szczególności z rozporządzeniem unijnym RODO oraz ustawą o ochronie danych osobowych;
c) przepisami dotyczącymi bezpieczeństwa narodowego.

§5
Zasady etyczne

1. Systemy AI powinny być wykorzystywane z poszanowaniem godności człowieka, praw podstawowych oraz zasad przejrzystości, odpowiedzialności i sprawiedliwości.
2. Zakazuje się stosowania AI w sposób prowadzący do inwigilacji, profilowania lub podejmowania decyzji automatycznych wobec pracowników, współpracowników lub studentów bez możliwości interwencji człowieka i bez właściwych regulacji wewnętrznych (np. Statut WAT, Regulamin Pracy, Regulamin Studiów), w których taki zakres stosowania byłby wprost określony.
3. Należy zapewnić, aby proces generowania treści odbywał się z poszanowaniem zasad uczciwości akademickiej, rzetelności, wiarygodności oraz osobistej odpowiedzialności za przedstawione informacje.
4. Autorzy prac, w tym prac powstałych z wykorzystaniem narzędzi sztucznej inteligencji ponoszą pełną odpowiedzialność za jakość merytoryczną przygotowanych treści oraz za skutki ich wykorzystania. Odpowiedzialność ta obejmuje także ewentualne, nieumyślne naruszenia przepisów prawa, w szczególności w zakresie ochrony praw autorskich oraz danych osobowych.
5. Niedopuszczalne jest wykorzystywanie treści o charakterze obraźliwym, dyskryminującym, niezgodnym z obowiązującym prawem lub mogących wprowadzać w błąd. W związku z powyższym, zaleca się systematyczne prowadzenie analiz materiałów generowanych z wykorzystaniem narzędzi sztucznej inteligencji – w tym tekstów, grafik, nagrań dźwiękowych, materiałów wideo i innych plików multimedialnych – oraz ich szczegółową weryfikację przed publikacją lub udostępnieniem w przestrzeni publicznej.
6. Autorstwo treści wygenerowanych przy użyciu narzędzi opartych na metodach sztucznej inteligencji – niezależnie od ich formy, w tym tekstów, algorytmów, oprogramowania, grafik czy utworów muzycznych – nie może być przypisywane

[1] 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) (Tekst mający znaczenie dla EOG) - https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1689

osobie korzystającej z tych narzędzi jako twórcy w rozumieniu prawa autorskiego. Dla zachowania rzetelności naukowej i dydaktycznej konieczne jest jednoznaczne wskazanie źródła oraz zakresu wykorzystania treści wygenerowanych przez sztuczną inteligencję.

§6
Bezpieczeństwo i poufność

1. Wszelkie wdrożenia AI muszą być poprzedzone udokumentowaną analizą ryzyka, a systemy AI wysokiego ryzyka wymagają dodatkowo zatwierdzenia przez Pełnomocnika Rektora ds. AI.
2. Dane wrażliwe nie mogą być przetwarzane przez systemy AI bez odpowiednich certyfikatów bezpieczeństwa.
3. Przetwarzanie informacji niejawnych przez systemy AI możliwe jest wyłącznie po spełnieniu wymagań określonych przez organizatora systemu niejawnego, w którym ten system AI został udostępniony.
4. Do użytku dopuszcza się wyłącznie te narzędzia AI, które nie wykorzystują danych wejściowych do dalszego uczenia się w sposób niekontrolowany, chyba że dane te są jawne, zgeneralizowane lub podlegają kontroli instytucjonalnej i zostały zatwierdzone przez Zespół ds. Etyki AI.
5. Należy brać pod uwagę, że interakcje z narzędziami opartymi na sztucznej inteligencji mogą nie mieć charakteru prywatnego, a wprowadzane zapytania oraz generowane odpowiedzi mogą być rejestrowane, analizowane i wykorzystywane przez podmioty trzecie, w tym dostawców tych technologii.

Rozdział III – AI w nauce

§7
Wykorzystanie AI w badaniach naukowych

1. AI może być stosowana w analizie danych, modelowaniu symulacyjnym, prognozowaniu, wykrywaniu zależności, optymalizacji procesów i innych formach badań z zachowaniem zasad dobrej praktyki naukowej oraz poszanowaniem zapisów odrębnych umów na realizację tych badań.
2. W publikacjach naukowych należy jawnie wskazywać, czy i w jaki sposób wykorzystywano narzędzia AI oraz ich rodzaj.
3. Każdy projekt badawczy z udziałem AI musi zawierać ocenę ryzyka, w tym technologicznego.

§8
AI w przygotowaniu publikacji naukowych

1. Dopuszcza się wspomaganie przygotowania publikacji naukowych z wykorzystaniem narzędzi AI, w szczególności do:
   a) redagowania tekstu (np. poprawa stylistyczna lub gramatyczna);
   b) tłumaczeń technicznych;
   c) generowania wykresów i wizualizacji na podstawie danych;
   d) analizy treści;
   e) sprawdzania spójności merytorycznej i logicznej.
2. Nie powinno się dopuszczać wykorzystania modeli językowych do doboru literatury i cytowań.

3. W każdym przypadku autor publikacji jest odpowiedzialny za końcowy kształt tekstu oraz jego oryginalność i zgodność z zasadami etyki naukowej.
4. W przypadku wykorzystania AI w przygotowaniu publikacji, zaleca się zawarcie stosownej informacji (np. *„W przygotowaniu tekstu wspomagano się narzędziem AI: [nazwa narzędzia]”*).
5. Zabronione jest generowanie całych artykułów naukowych przez AI bez nadzoru i wkładu intelektualnego autora.

§9
Odpowiedzialność badawcza

Kierownik projektu badawczego ponosi odpowiedzialność za właściwe zastosowanie AI, w tym za zapewnienie jakości danych oraz interpretację wyników.

Rozdział IV – AI w dydaktyce

§10
Wsparcie dydaktyki przez AI

1. AI może być wykorzystywana do personalizacji nauczania, analizy postępów studentów, tworzenia materiałów dydaktycznych oraz wsparcia procesu oceniania.
2. Wykorzystanie narzędzi sztucznej inteligencji nie może prowadzić do ograniczenia roli nauczyciela akademickiego w procesie dydaktycznym ani do wdrażania zautomatyzowanych form nadzoru nad studentami, które mogłyby naruszać zasady autonomii akademickiej oraz relacji „mistrz–uczeń”.
3. Wykorzystanie narzędzi sztucznej inteligencji nie może zastępować bezpośredniego kontaktu dydaktycznego pomiędzy nauczycielem akademickim a studentem, chyba że forma prowadzenia zajęć przewiduje taką możliwość zgodnie z obowiązującym programem kształcenia.

§11
Zasady transparentności

1. Studenci muszą być informowani o zastosowaniu AI w procesie dydaktycznym.
2. Informacje, o których mowa w ust. 1, powinny być przedstawione uczestnikom zajęć w sylabusie (karcie informacyjnej przedmiotu) oraz omówione podczas pierwszych zajęć.
3. Każdy student ma prawo odmówić udziału w procesie dydaktycznym opartym wyłącznie na wykorzystaniu AI, który całkowicie zastępuje bezpośrednią interakcję z wykładowcą, bez konsekwencji dla toku studiów.
4. Nauczyciele akademiccy zobowiązani są do kontroli i oceny wykorzystania AI przez studentów.

§12
Wykorzystanie AI przez studentów

1. Wykorzystanie narzędzi AI przy pisaniu prac dyplomowych, końcowych lub etapowych (sprawozdań, prezentacji, prac zaliczeniowych, egzaminacyjnych, itp.) może mieć miejsce jedynie za zgodą promotora/prowadzącego zajęcia.
2. W przypadku użycia narzędzi AI w pracy dyplomowej, końcowej lub etapowej, promotor/prowadzący zajęcia ma obowiązek:

a) określenia rodzaju wykorzystywanych narzędzi oraz sposobów, celów i zakresu zastosowania AI;
b) określenia sposobu oznaczania treści wygenerowanych przez AI;
c) monitorowania postępów studenta w sposób pozwalający na weryfikację efektów uczenia się oraz oceny indywidualnego wkładu studenta w efekty końcowe ocenianych prac.

3. W każdej pracy dyplomowej, końcowej lub etapowej, w której użyto narzędzi AI, należy zawrzeć informację (np. we wstępie) zawierającą w szczególności:
   a) nazwę użytego narzędzia,
   b) zakres jego wykorzystania,
   c) stopień wpływu na ostateczną formę pracy.
4. W przypadku pracy dyplomowej, końcowej lub etapowej wytworzonej bez użycia narzędzi AI, obowiązuje oświadczenie: *„Oświadczam, że praca została wytworzona samodzielnie i bez wykorzystania narzędzi AI”*.
5. Niedozwolone jest wykorzystywanie narzędzi sztucznej inteligencji do generowania treści prac dyplomowych, końcowych lub etapowych w sposób eliminujący istotny, samodzielny wkład autora. Wszelkie zastosowanie AI musi mieć charakter wspomagający i nie może zastępować procesu twórczego, analitycznego ani decyzyjnego studenta.
6. Podczas zaliczeń i egzaminów, zarówno w trybie stacjonarnym, jak i zdalnym, użycie AI jest zakazane, chyba że zasady zaliczenia przedmiotu stanowią inaczej. W takim przypadku użycie AI musi być wyraźnie określone.
7. Prace dyplomowe, końcowe lub etapowe mogą być weryfikowane pod kątem nieujawnionego użycia systemów AI za pomocą detektorów AI, a autor pracy zobowiązany jest do poddania się tej procedurze.
8. Każde naruszenie niniejszych zasad może skutkować odpowiedzialnością dyscyplinarną zgodnie ze Statutem WAT i Regulaminem Studiów.
9. W przypadku stwierdzenia nieujawnionego stosowania narzędzi opartych na sztucznej inteligencji promotor/prowadzący zajęcia powinien zawiadomić o tym w formie pisemnej osobę kierującą Wydziałem.

Rozdział V – AI w administracji uczelni

§13
Automatyzacja procesów administracyjnych

1. Systemy AI mogą wspierać zarządzanie dokumentacją, komunikację, planowanie zasobów oraz obsługę studentów i pracowników.
2. Wdrażane systemy muszą spełniać wymogi interoperacyjności, audytowalności i ochrony prywatności.

§14
Nadzór i audyt

Wszystkie wdrażane systemy AI stosowane w administracji podlegają corocznemu audytowi wewnętrznemu z udziałem Inspektora Ochrony Danych oraz Pełnomocnika ds. AI.

Rozdział VI – Organy i odpowiedzialność

§15

Pełnomocnik Rektora ds. AI

Rektor w drodze decyzji powołuje Pełnomocnika ds. AI odpowiedzialnego za koordynację polityki AI, opiniowanie wdrożeń, audyt wewnętrzny systemów AI oraz edukację w zakresie etycznego stosowania AI.

§16

Zespół ds. Etyki AI

1. Zespół ds. Etyki AI (dalej Zespół) składający się z przedstawicieli kadry naukowej, administracji, studentów oraz Działu Informatyki ocenia zgodność projektów AI z regulaminem i wydaje rekomendacje dla Rektora.
2. Zespół powoływany jest doraźnie przez Pełnomocnika Rektora ds. AI i działa pod jego przewodnictwem.
3. Stałymi członkami Zespołu są: Pełnomocnik Rektora ds. AI, przedstawiciel Działu Informatyki, Inspektor Ochrony Danych oraz Pełnomocnik Rektora ds. Bezpieczeństwa Informacji.
4. Ocena zgodności projektu AI, o którym mowa w ust. 1 nie może zostać dokonana bez udziału w Zespole przedstawiciela jednostek organizacyjnych lub studentów, których ten projekt dotyczy.

Rozdział VII – Wytyczne dla własnych systemów AI

§17

Wymagania ogólne

1. Wszelkie systemy sztucznej inteligencji opracowywane lub rozwijane w WAT muszą spełniać standardy bezpieczeństwa, etyki oraz być zgodne z obowiązującymi normami i krajowym ustawodawstwem.
2. Przed rozpoczęciem projektowania systemu AI należy przeprowadzić:
   a) ocenę wpływu technologii – jak system AI może wpłynąć na ludzi, społeczeństwo, środowisko, rynek pracy, prywatność czy prawa człowieka, tj. przewidzieć potencjalne skutki (zarówno pozytywne, jak i negatywne) związane z wdrożeniem tej technologii;
   b) analizę ryzyka – proces identyfikowania i oceniania możliwych zagrożeń związanych z działaniem AI, takich jak błędy w podejmowaniu decyzji, uprzedzenia algorytmu (bias), problemy z bezpieczeństwem danych, awarie, czy niewłaściwe użycie systemu.
3. Wdrożenie systemu w WAT wymaga zaopiniowania przez Zespół ds. Etyki AI.

§18

Zabezpieczenia techniczne i przeciwdziałanie atakom adwersarialnym

1. Systemy AI muszą zawierać mechanizmy uniemożliwiające zewnętrznym podmiotom:
   a) modyfikowanie decyzji modelu poprzez ataki adwersarialne (np. wstrzykiwanie danych wejściowych w celu zmanipulowania odpowiedzi);

b) przeprowadzanie ataków typu *model inversion*, *membership inference* oraz innych metod prowadzących do rekonstrukcji logiki działania modelu lub danych uczących.

2. Wymaga się stosowania technik takich jak:
   a) wzmacnianie odporności modelu;
   b) wprowadzanie mechanizmów detekcji i neutralizacji podejrzanych zapytań;
   c) izolacja komponentów przetwarzających dane wejściowe.
3. Każdy system AI narażony na ataki adwersarialne musi posiadać warstwę audytu i monitoringu umożliwiającą śledzenie aktywności użytkowników oraz nietypowych zachowań systemu.

§19
Dane treningowe – ochrona, jakość i weryfikacja

1. Wszystkie dane wykorzystywane do uczenia modeli AI muszą pochodzić z legalnych i kontrolowanych źródeł, być zgodne z profilem bezpieczeństwa.
2. Dane należy poddawać:
   a) procesowi anonimizacji (jeśli dotyczą osób fizycznych);
   b) walidacji merytorycznej (zgodność z przeznaczeniem systemu);
   c) analizie wykrywania błędów, stronniczości oraz niepożądanych korelacji.
3. Niedozwolone, z zastrzeżeniem ust. 4, jest wykorzystywanie danych:
   a) niejawnych;
   b) niezweryfikowanych (ich pochodzenie, jakość lub zgodność z rzeczywistością nie zostały potwierdzone);
   c) pozyskanych z systemów o nieznanej infrastrukturze bezpieczeństwa.
4. Jeżeli celem tworzenia systemu AI jest analiza/przetwarzanie danych, o których mowa w ust. 3 lit. b i c wymagana jest opinia Zespołu ds. Etyki AI.
5. Niedozwolone jest wykorzystanie danych w sposób naruszający licencje lub prawa autorskie.

§20
Procesy walidacyjne i audytowe

1. Każdy system AI podlega okresowej weryfikacji:
   a) przed wdrożeniem (walidacja przedeksploatacyjna);
   b) w czasie eksploatacji (ciągłe testy spójności i dokładności);
   c) po istotnych aktualizacjach (walidacja rekonfiguracyjna).
2. Pełnomocnik Rektora ds. AI może zlecić audyt systemu AI. Audyt przeprowadza zespół interdyscyplinarny, w skład którego wchodzą specjaliści z zakresu technologii AI, specjaliści z zakresu bezpieczeństwa teleinformatycznego, analitycy ryzyka, przedstawiciele władz WAT oraz administratorzy danych.
3. Systemy, które nie spełniają wymagań audytowych, podlegają natychmiastowemu wstrzymaniu działania lub ograniczeniu dostępności do czasu wyeliminowania niezgodności.

Rozdział VIII – Identyfikacja i zarządzanie ryzykami systemów AI

§21

Reagowanie na cyberzagrożenia

1. WAT wdraża efektywny i adaptowalny system reagowania na incydenty bezpieczeństwa związane z systemami AI, obejmujący:
   a) detekcję anomalii i ataków cybernetycznych w czasie rzeczywistym;
   b) automatyczne procedury ograniczenia dostępu w przypadku wykrycia naruszeń;
   c) gotowe scenariusze reagowania operacyjnego (ang. *incident response playbooks*);
   d) ćwiczenia symulacyjne dla zespołów IT i administracji.
2. W przypadku wystąpienia incydentu zastosowanie mają postanowienia Polityki Bezpieczeństwa Informacji.

§22

Zarządzanie cyklem życia systemów AI

1. Każdy system AI wdrażany lub planowany do wdrożenia w WAT musi przejść formalny cykl zarządzania, który obejmuje:
   a) etap projektowania i analizy zagrożeń;
   b) etap wdrażania i testowania zgodności;
   c) etap eksploatacji i ciągłego monitorowania;
   d) etap wycofania systemu lub jego migracji.
2. Za zarządzanie cyklem życia odpowiada jednostka wdrażająca oraz Pełnomocnik ds. AI w porozumieniu z Działem Informatyki.

§23

Zapobieganie manipulacjom i dezinformacji

1. Systemy AI nie mogą być wykorzystywane do:
   a) generowania lub rozpowszechniania niezweryfikowanych treści;
   b) automatyzacji tworzenia wiadomości o charakterze politycznym, ideologicznym lub propagandowym;
   c) wpływania na decyzje pracowników lub studentów poprzez manipulację informacyjną.
2. Wszelkie systemy zdolne do generowania treści muszą mieć funkcje oznaczania treści jako wygenerowane przez AI.
3. Zastosowanie AI w komunikacji zewnętrznej musi zostać zaopiniowane przez Rzecznika Prasowego WAT oraz Zespół ds. Etyki AI.

§24

Ryzyko naruszenia prywatności

1. Systemy AI nie mogą przetwarzać danych osobowych bez przesłanki legalizującej przetwarzanie danych osobowych zgodnej z art. 6 ust. 1 RODO.
2. Przetwarzanie danych osobowych z wykorzystaniem AI musi być zgodne z zasadami przetwarzania danych osobowych opisanych w art. 5 RODO oraz Polityką Bezpieczeństwa Informacji.

3. Wymagane jest stosowanie zasad *privacy-by-design* i *privacy-by-default* w każdym projekcie AI, co oznacza konieczność analizy ryzyka naruszenia praw lub wolności osób fizycznych.
4. Dane muszą być odpowiednio zabezpieczone, pseudonimizowane lub anonimizowane, a dostęp do nich limitowany do niezbędnego minimum. W zapytaniach nie powinno używać się rzeczywistych danych osobowych (np. imion, nazwisk, identyfikatorów, zdjęć).

§25
Interpretowalność modeli

1. Niedopuszczalne jest podejmowanie decyzji wpływających na prawa lub obowiązki osób fizycznych wyłącznie w oparciu o systemy AI, których działania nie można wyjaśnić.
2. Preferowane są modele transparentne lub oparte na zasadzie XAI *(Explainable AI)*.
3. W przypadku stosowania modeli o ograniczonej interpretowalności, wymagane jest:
   a) prowadzenie dokumentacji testowej i operacyjnej;
   b) stosowanie narzędzi do interpretacji wyników (np. LIME, SHAP);
   c) zapewnienie możliwości interwencji człowieka na każdym etapie procesu decyzyjnego.

Rozdział IX – Edukacja i rozwój kompetencji w zakresie AI

§26
Obowiązek rozwoju kompetencji

Wszyscy pracownicy są zobowiązani do systematycznego podnoszenia wiedzy z zakresu:
1. działania i ograniczeń systemów AI;
2. zasad ich etycznego i bezpiecznego stosowania;
3. zagrożeń związanych z cyberbezpieczeństwem oraz dezinformacją;
4. interpretacji wyników generowanych przez systemy AI.

§27
Programy szkoleń i certyfikacji

1. Pełnomocnik ds. AI organizuje cykliczne szkolenia, warsztaty oraz kursy e-learningowe z zakresu AI – obowiązkowe dla wszystkich użytkowników, którym udostępnione będą narzędzia AI oraz zalecane dla wszystkich pracowników.
2. Dla stanowisk, które bezpośrednio nadzorują, tworzą lub eksploatują systemy AI, wymagana jest certyfikacja wewnętrzna (lub zewnętrzna, zgodnie z rekomendacją Pełnomocnika ds. AI).
3. WAT może zawierać porozumienia z instytucjami zewnętrznymi w celu wspólnego rozwoju kompetencji AI.
4. WAT zapewnia dostęp do artykułów, nagrań i szkoleń oraz raportów na temat AI poprzez ich umieszczenie na portalu intranetowym lub platformie e-learningowej.

§28
Monitorowanie wiedzy i wsparcie rozwoju

1. Pełnomocnik Rektora ds. AI prowadzi monitoring udziału pracowników w szkoleniach oraz opracowuje coroczny raport nt. poziomu przygotowania pracowników do pracy z systemami AI.
2. Pełnomocnik Rektora ds. AI jest koordynatorem wsparcia w zakresie doradztwa technicznego, konsultacji etycznych oraz dostępu do materiałów edukacyjnych.
3. Niewypełnianie obowiązku szkoleniowego może skutkować ograniczeniem dostępu do systemów AI lub projektów badawczych wykorzystujących AI.