URZĄD PATENTOWY
RZECZYPOSPOLITEJ POLSKIEJ

POLITYKA AI
URZĘDU PATENTOWEGO RZECZYPOSPOLITEJ POLSKIEJ

Wersja: 1.0

Metryka dokumentu

URZĄD PATENTOWY RZECZYPOSPOLITEJ POLSKIEJ					
Dokument	Polityka AI Urzędu Patentowego Rzeczypospolitej Polskiej				
Krótki opis dokumentu	Dokument określa zbiór zasad i wytycznych operacyjnych, wskazujących w jaki sposób technologia sztucznej inteligencji może być bezpiecznie, etycznie i zgodnie z prawem wykorzystywana wewnątrz Urzędu Patentowego RP. Dokument ten definiuje dopuszczalne narzędzia, zakres stosowania AI oraz standardy ochrony danych, zapewniając ramy dla odpowiedzialnego korzystania z tej technologii w codziennej pracy.				
Właściciel dokumentu	Urząd Patentowy Rzeczypospolitej Polskiej				
Komórka odpowiedzialna za opracowanie dokumentu	Zespół do spraw sztucznej inteligencji				
Opracowanie	Marek Gajewski – Naczelnik w Departamencie Informatyki Lidia Aleksandrowicz – Główny Specjalista w Departamencie Prawnym i Orzecznictwa Tomasz Müller – Ekspert Koordynator w Departamencie Zgłoszeń Jarosław Żak – Ekspert w Departamencie Elektroniki i Mechaniki Krzysztof Paruch – Ekspert w Departamencie Znaków Towarowych	Data	18.05.2026	Podpis	/ podpisano elektronicznie /
Zatwierdzenie	Ewa Skrzydło-Tefelska – Prezes Urzędu Patentowego Rzeczypospolitej Polskiej	Data	18.05.2026	Podpis	/ podpisano elektronicznie /
Data druku	18.05.2026		Liczba stron		18
Nazwa pliku	Polityka_AI_wersja_1_0.docx		Status dokumentu*		Z

(*) Status dokumentu: O – opracowywany, Z – Zatwierdzony, Z/A – Zatwierdzony i zaktualizowany, X – Odwołany

Historia zmian

Nr wersji	Data	Opis	Działanie (*)	Rozdziały (**)	Autorzy
1.0	18.05.2026	Utworzenie nowego dokumentu i uwzględnienie uwag	N	W	Marek Gajewski Lidia Aleksandrowicz Tomasz Müller Jarosław Żak Krzysztof Paruch

(*) Działanie: N-Nowy, Z-Zmiana, We-Weryfikacja
(**) Rozdziały: numery rozdziałów lub W-Wszystkie

Spis treści

1. Cel polityki AI

Współczesny rozwój technologii cyfrowych ma coraz większy wpływ na życie społeczne, w tym również na funkcjonowanie administracji publicznej. Aby odpowiadać na potrzeby społeczeństwa, administracja musi dostosowywać swoje funkcje i struktury nie tylko do zmian prawnych, ale również społecznych i technologicznych.

Celem Polityki AI jest określenie zasad świadomego i odpowiedzialnego korzystania z narzędzi AI w Urzędzie Patentowym RP w pełnej zgodzie z obowiązującymi przepisami prawa, aby Urząd korzystał z dynamicznego rozwoju Sztucznej Inteligencji przy zachowaniu nadrzędnej roli człowieka.

2. Zakres polityki AI

Polityka AI obejmuje wszystkich użytkowników systemów sztucznej inteligencji we wszystkich obszarach merytorycznych i administracyjnych Urzędu. Dokument ten określa ramy świadomego i odpowiedzialnego korzystania z narzędzi AI, wskazując zarówno na szanse, jakie oferuje ta technologia, jak i na powiązane z nią ryzyka. W szczególności polityka reguluje kwestie ewidencji narzędzi, ochrony poufności danych (ze szczególnym uwzględnieniem danych nieopublikowanych) oraz obowiązkowej weryfikacji wyników generowanych przez AI w celu zapewnienia bezpieczeństwa prawnego i etycznego.

3. Słownik pojęć

W tej części opisujemy znaczenie podstawowych pojęć związanych ze sztuczną inteligencją, jej podstawowymi błędami i ograniczeniami oraz wyjaśniamy jak rozumiemy kluczowe hasła używane w Polityce AI. Zrozumienie tych pojęć jest niezbędne do odpowiedzialnego i bezpiecznego stosowania sztucznej inteligencji w Urzędzie, dlatego celem opisów jest zapewnienie wspólnego rozumienia terminów związanych ze sztuczną inteligencją, a nie przywołanie ścisłych definicji.

Sztuczna inteligencja (ang. Artificial Intelligence, w skrócie AI) to dziedzina informatyki, zajmująca się tworzeniem oprogramowania wykonującego czynności, których wykonanie przez człowieka wymagałoby posłużenia się inteligencją, np. rozumienie języka czy rozwiązywanie problemów.

Wyjaśnialna AI (ang. explainable AI, w skrócie XAI) to technologia AI, potrafiąca podać argumenty, które objaśniają podjętą przez AI decyzję, w efekcie czego użytkownicy widzą nie tylko wynik, ale i jego uzasadnienie lub kontekst.

Generatywna sztuczna inteligencja AI (ang. generative AI, w skrócie GenAI) to termin, którym możemy określać formę sztucznej inteligencji tworzącą, na podstawie danych, którymi była trenowana, nowe treści (np. teksty, obrazy).

Wielki model językowy (LLM) (ang. Large Language Model, w skrócie LLM) to zaawansowany system AI, wyspecjalizowany w przetwarzaniu informacji tekstowych. Został wytrenowany na podstawie analizy ogromnych zasobów dokumentów i danych publicznych, co pozwala mu na sprawne redagowanie pism, streszczanie złożonych materiałów oraz precyzyjne odpowiadanie na zapytania. Działanie LLM nie opiera się na sztywnych regułach, lecz analizie kontekstu wypowiedzi i dobraniu najbardziej prawdopodobnych sformułowań, naśladując naturalny sposób komunikacji człowieka.

System AI to system komputerowy, który działa częściowo samodzielnie, potrafi uczyć się na podstawie danych w celu wypracowania propozycji analiz statystycznych, rekomendacji merytorycznych oraz treści tekstowych, graficznych lub video.

Shadow AI jest zjawiskiem wykorzystania narzędzi AI w trakcie pracy bez wiedzy i zgody pracodawcy, mogącym prowadzić np. do ujawnienia na zewnątrz danych poufnych.

Human-in-the-loop (HITL) to koncepcja współpracy człowieka z systemami AI, w której człowiek zachowuje rzeczywistą kontrolę w procesie decyzyjnym w ramach nadzoru, korekty i zatwierdzania wyników działania systemów AI. Koncepcja ta zakłada wykorzystanie ludzkiej wiedzy eksperckiej na kluczowych etapach w trakcie weryfikacji i ewentualnej poprawy wyników działania systemu.

Prompt jest instrukcją lub pytaniem tekstowym, które użytkownik wprowadza do modelu AI sugerując, jaką chciałby uzyskać odpowiedź.

Halucynacja to zjawisko, gdy model AI generuje informacje brzmiące wiarygodnie, jednak będące nieprawidłowe, zmyślone lub nie mające podstaw w rzeczywistości. Model nie sygnalizuje przy tym, że podaje fałszywe dane.

Bias - (ang. „uprzedzenie", „stronniczość") to systematyczne odchylenie od neutralności lub obiektywizmu wyników systemu AI. Taka sytuacja będzie miała miejsce, gdy dane treningowe systemu AI były niezrównoważone, model uczył się na niewłaściwie dobranych danych, wskutek czego algorytm faworyzował będzie jedne rozwiązania kosztem innych.

4. Ochrona prawna

Tworzenie i wykorzystywanie sztucznej inteligencji podlega przepisom prawa, zarówno krajowego jak i międzynarodowego. Dotyczy to w szczególności: ochrony praw człowieka i dóbr osobistych, ochrony danych osobowych oraz zasad uczciwej konkurencji, prawa cywilnego, administracyjnego i karnego oraz własności intelektualnej (prawa autorskie, prawa własności przemysłowej).

Projektując i wdrażając rozwiązania AI, działamy z poszanowaniem praw podstawowych, w tym:

- prawa do prywatności i ochrony danych osobowych[1];
- godności człowieka, wolności, demokracji, równości, niedyskryminacji i sprawiedliwości[2].

Pracujemy nad rozwiązaniami, które są zgodne z przepisami rozporządzenia Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sztucznej inteligencji, zwanego dalej: „AI Act”[3], nie uchybiając w tym innym przepisom, w szczególności dotyczącym:

- ochrony danych osobowych;
- ochrony informacji niejawnych;
- zwalczania nieuczciwej konkurencji;
- postępowania administracyjnego;
- prawa własności przemysłowej[4].

[1] art. 51 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. nr 78, poz. 483 z późn. zm.) oraz art. 8 Karty praw podstawowych UE (Dz.Urz.UE.C 2010 Nr 83, str. 389)
[2]art. 2 Traktatu o Unii Europejskiej (Dz.Urz.UE.C 2012 Nr 326, str. 13)
[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 w sprawie zharmonizowanych przepisów dotyczących sztucznej inteligencji (Dz.Urz.UE.L z 2024 r. str. 1689) (Rozporządzenie AI ACT)
[4] 1) Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych) (Dz.Urz.UE.C 2016 Nr L119, str. 1) (RODO); 2) u stawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 2025 r. poz 1691) (KPA); 3) ustawa z dnia 30 czerwca 2000 r. Prawo własności przemysłowej (Dz.U. z 2023 r. poz. 1170) (PWP), w tym przepisy dotyczące ochrony nowości wynalazków (art. 25) oraz procedur rejestracji praw wyłącznych; 4) ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2025 r. poz. 1209); 5) ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2026 r. poz. 85) – w zakresie ochrony tajemnicy przedsiębiorstwa.

Poszanowanie powyższych przepisów i zasad ma dla nas szczególne znaczenie ze względu na charakter zadań Urzędu jako organu powołanego m.in. do udzielania ochrony prawnej na przedmioty własności przemysłowej. Przy korzystaniu z narzędzi AI uwzględniamy specyfikę udzielanych praw, w tym wymogi poufności zgłoszeń przed ich publikacją, ochronę danych osobowych zgłaszających, uprawnionych i twórców oraz konieczność zapewnienia, że decyzje Urzędu są podejmowane przez eksperta, a nie przez algorytm.

5. Świadome i odpowiedzialne korzystanie z narzędzi AI

5.1. Ewidencja i kategoryzacja narzędzi

Prowadzimy Rejestr Narzędzi AI, który zawiera wykaz systemów sztucznej inteligencji dopuszczonych do stosowania w Urzędzie:

- Rejestr jest jawny dla pracowników i na bieżąco aktualizowany.
- Rejestr stanowi oficjalny wykaz Narzędzi Autoryzowanych, zapewniając pracownikom jasne wytyczne w zakresie bezpiecznego i zgodnego z regulacjami wykorzystania systemów AI.

Przy doborze i ocenie narzędzi AI uwzględnia się kierunki rozwoju technologicznego określone w dokumentach strategicznych Urzędu.

5.1.1. Kategorie narzędzi

Narzędzia AI dzielimy na dwie kategorie:

1) **Narzędzia Autoryzowane** – systemy AI i funkcjonalności AI wpisane do Rejestru. Dane wprowadzane do tych systemów nie są wykorzystywane do trenowania modeli publicznych, co zapewnia ochronę tajemnicy zgłoszeń oraz tajemnicy przedsiębiorstwa zgłaszających. Mogą to być zarówno narzędzia wewnętrzne (np. wbudowane w systemy urzędowe), jak i zewnętrzne (np. specjalistyczne narzędzia do klasyfikacji patentowej).
2) **Narzędzia Nieautoryzowane** – systemy AI niewpisane do Rejestru, w tym rozwiązania ogólnodostępne oraz testowe. Ich wykorzystanie jest dopuszczalne wyłącznie w zakresie zadań niewymagających przetwarzania danych prawnie chronionych, tj. danych krytycznych, wrażliwych lub ograniczonych, zgodnie z zasadami określonymi w pkt 5.2.

5.1.2. Zawartość Rejestru

Rejestr Narzędzi AI zawiera dla każdego narzędzia autoryzowanego co najmniej:

1) nazwę i wersję narzędzia;
2) dostawcę lub producenta;
3) kategorię ryzyka;

4) dopuszczalne kategorie danych zgodnie z klasyfikacją określoną w strategii AI (dane krytyczne, wrażliwe, ograniczone, publiczne) oraz zbiory danych;
5) przeznaczenie;
6) warunki stosowania, w tym wymogi dotyczące oznaczania treści wygenerowanych przez AI;
7) właściciela biznesowego narzędzia;
8) status (np. wdrożone, w testach, w weryfikacji);
9) typ środowiska (on-premise, zaufana chmura z izolacją, chmura publiczna).

5.2. Ochrona danych i poufności, w tym danych nieopublikowanych

Na potrzeby niniejszej Polityki stosujemy klasyfikację danych określoną w Strategii AI Urzędu Patentowego RP (pkt 3.1), która wyodrębnia cztery kategorie: dane krytyczne, wrażliwe, ograniczone, publiczne. Zasady przetwarzania danych poszczególnych kategorii w systemach AI określa Strategia AI (pkt 3.2-3.3).

Nie wprowadzamy do narzędzi nieautoryzowanych danych krytycznych ani danych wrażliwych w rozumieniu Strategii AI, w szczególności danych osobowych, informacji służbowych, treści dotyczących zgłoszeń oraz innych materiałów wrażliwych. W przypadku narzędzi nieautoryzowanych, z ostrożności przyjmujemy założenie, że wszystkie dane wpisane w pole konwersacji zostaną wykorzystane do trenowania modeli AI i staną się publicznie dostępne.

Dane ograniczone i dane publiczne mogą być przetwarzane w narzędziach nieautoryzowanych wyłącznie na warunkach określonych w Strategii AI (pkt 3.3), tj. pod warunkiem, że nie mają charakteru informacji niejawnych ani tajemnicy przedsiębiorstwa, przetwarzanie odbywa się w zakresie niezbędnym do realizacji zadań Urzędu, a pracownik każdorazowo dokonał oceny ryzyka związanego z przekazaniem danych. W razie wątpliwości pracownik rezygnuje z wprowadzenia danych.

Narzędzi nieautoryzowanych nie wykorzystujemy do przetwarzania nieupublicznionych informacji złożonych do akt sprawy.

Korzystając z narzędzi AI, kierujemy się zasadami:

- **minimalizacji danych**, wprowadzając do narzędzia AI tylko te dane, które są niezbędne do realizacji zadania;
- **anonimizacji i pseudonimizacji danych** przed wprowadzeniem ich do narzędzia AI, jeśli ich podanie nie jest konieczne do uzyskania wyniku;
- **odpowiedzialności** za wprowadzenie danych chronionych poprzez zgłaszanie incydentów w ramach potencjalnych ujawnień.

5.3. Weryfikacja wyników AI

Każdy wynik wygenerowany przez system AI traktujemy jako pomocniczy i krytycznie weryfikujemy przed wykorzystaniem. Przeciwdziałamy tendencji do automatycznego polegania na wynikach AI - unikamy tzw. błędu automatyzacji (ang. automation bias), czyli skłonności do nadmiernego zaufania wynikom generowanym przez system AI. Kierujemy się zasadą, że każdy pracownik może zignorować lub skorygować wynik wygenerowany przez system AI, jeśli uzna to za uzasadnione. Decyzja administracyjna oraz inne dokumenty wywołujące skutki prawne są bowiem aktem woli człowieka, poprzedzonym wyczerpującym wyjaśnieniem stanu faktycznego. Niedopuszczalne jest oparcie rozstrzygnięcia wyłącznie na wyniku zautomatyzowanego przetwarzania.

Wszelkie treści wygenerowane przez systemy AI muszą zostać poddane weryfikacji merytorycznej w oparciu o wiarygodne źródła. W ramach tego procesu pracownik jest zobowiązany do każdorazowego sprawdzenia następujących aspektów:

1) **faktów i danych** – czy informacje są zgodne ze stanem rzeczywistym i aktualne;
2) **podstaw prawnych** – czy powoływane przepisy istnieją, są prawidłowo przytoczone i obowiązują w aktualnym brzmieniu (weryfikacja bezpośrednio w ustawach, w Systemie Informacji Prawnej, bazie ISAP lub EUR-Lex, itp.);
3) **orzecznictwa i literatury** – czy przywołane wyroki, decyzje lub publikacje rzeczywiście istnieją;
4) **dokumentów ze stanu techniki** – czy wskazane patenty, zgłoszenia lub publikacje naukowe są dostępne w wiarygodnych bazach danych (np. Espacenet, Register Plus, bazy literatury niepatentowej);
5) **spójności i logiki** – czy treść jest wewnętrznie spójna i odpowiada na właściwe pytanie (ocena merytoryczna pracownika);
6) **kompletności** – czy system AI nie pominął istotnych fragmentów dokumentacji źródłowej mających znaczenie dla sprawy;
7) **wiarygodności merytorycznej** – czy treść jest wolna od halucynacji AI, czyli zmyślonych faktów, dat lub przepisów prawa;
8) **bezstronności** – czy sugestia AI wydaje się nietypowa lub traktuje podobne przypadki w różny sposób, niezgodnie z dotychczasową praktyką Urzędu.

Niedopuszczalne jest:

1) bezpośrednie przenoszenie treści wygenerowanych przez AI do decyzji, postanowień lub innych dokumentów urzędowych bez uprzedniej merytorycznej weryfikacji i redakcji;

2) powoływanie się na orzecznictwo, literaturę lub dokumenty patentowe, których treści nie zweryfikowano;
3) wykorzystywanie wyników AI jako ostatecznej oceny w sprawach wymagających szczególnej precyzji i oceny eksperckiej (np. ocena nowości wynalazku, ocena poziomu wynalazczego, ocena charakteru odróżniającego znaku towarowego, ocena indywidualnego charakteru wzoru przemysłowego).

5.4. Transparentność

Zapewnienie transparentności w wykorzystaniu sztucznej inteligencji jest kluczowym aspektem realizacji zadań publicznych przez Urząd. Osoby fizyczne, których dotyczą procesy wspierane przez AI, są o tym fakcie informowane w sposób jasny i zrozumiały. Obowiązek ten jest realizowany w szczególności w następujących sytuacjach:

- Jeśli podejmując decyzję dotyczącą interesów prawnie chronionych osoby fizycznej zastosujemy system AI wysokiego ryzyka, poinformujemy osobę, której decyzja dotyczy o wykorzystaniu w stosunku do niej systemu AI[5]. Osoba taka ma prawo zwrócenia się do Urzędu o wyjaśnienie w sposób jasny i merytoryczny roli systemu AI w procesie podejmowania względem niej konkretnej decyzji[6].
- Jeśli posłużymy się systemem AI, który będzie generował obrazy, treści audio lub wideo poinformujemy, już przy pierwszym wyświetleniu, że przedstawione treści zostały sztucznie wygenerowane lub zmanipulowane przy użyciu AI[7].
- Jeśli posłużymy się z systemem AI, który będzie wchodził w bezpośrednią interakcję z osobą fizyczną poinformujemy tę osobę o tym, że prowadzi interakcję z systemem sztucznej inteligencji. Informacja taka zostanie przekazana w sposób jasny i wyraźny już w momencie nastąpienia pierwszej interakcji[8].

5.5. Etyka

Wykorzystanie systemów sztucznej inteligencji opiera się na zasadzie odpowiedzialnego przetwarzania danych. Jako instytucja zaufania publicznego, zobowiązujemy się do zachowania najwyższych standardów etycznych w procesie trenowania, wdrażania i interpretacji wyników AI.

[5] art. 26 ust. 11 Rozporządzenia AI Act
[6] art. 86 ust. 1 Rozporządzenia AI Act
[7] art. 50 ust. 4 i 5 Rozporządzenia AI Act
[8] art. 50 ust. 4 i 5 Rozporządzenia AI Act

Jako organ administracji publicznej działamy zgodnie z prawem[9], prowadząc postępowania w sposób budzący zaufanie jego uczestników do władzy publicznej, kierując się zasadami proporcjonalności, bezstronności i równego traktowania[10].

Kluczową rolę w załatwianiu spraw w Urzędzie zawsze odgrywa człowiek. Systemy AI projektujemy, wdrażamy i rozwijamy tak, aby mogły być skutecznie nadzorowane przez pracowników. Nadzór ten ma zapobiegać ryzykom i zapewniać zgodność realizacji zadań z prawem, przy czym jego zakres jest współmierny do ryzyka, stopnia autonomii i sposobu użycia danego systemu AI[11].

Pracownicy korzystający z narzędzi AI są świadomi zjawiska błędu automatyzacji (ang. automation bias), czyli skłonności do nadmiernego zaufania wynikom generowanym przez systemy komputerowe[12]. Szczególną ostrożność zachowują, gdy:

- wynik AI wydaje się wiarygodny, ale dotyczy dziedziny wymagającej specjalistycznej wiedzy;
- system AI generuje odpowiedź z dużą pewnością, mimo niepełnych danych wejściowych;
- treść ma być wykorzystana w decyzji administracyjnej, opinii lub innym piśmie wydawanym w prowadzonym postępowaniu.

W przypadku wystąpienia wątpliwości pracownicy mają obowiązek zignorować wynik generowany przez AI i oprzeć rozstrzygnięcie na własnej analizie oraz źródłach pierwotnych[13].

[9] art. 6 KPA
[10] art. 8 KPA
[11] art. 14 ust 1-3 Rozporządzenia AI ACT
[12] art. 14 ust. 4 lit. b Rozporządzenia AI ACT
[13] art. 14 ust. 4 lit. d Rozporządzenia AI ACT

6. Kategoryzacja oraz obsługa incydentów

Stosujemy rygorystyczne standardy nadzoru nad systemami sztucznej inteligencji. W przypadku wykrycia nieprawidłowości, uruchamiamy ustandaryzowany proces zarządzania zdarzeniem:

- **Raportowanie zdarzenia** - promujemy kulturę odpowiedzialności, w której każde, nawet potencjalne odstępstwo od przyjętej Polityki AI, jest niezwłocznie zgłaszane do odpowiednich komórek nadzorczych, aby kompleksowo obsłużyć incydent (np. jednoczesne naruszenie Polityki AI oraz RODO). Umożliwia to natychmiastową reakcję i minimalizację ewentualnych ryzyk już w momencie ich wystąpienia.
- **Identyfikacja i powstrzymanie** - na tym etapie dokonujemy precyzyjnej diagnozy charakteru zdarzenia oraz – jeśli to konieczne – podejmujemy szybkie działania techniczne w celu odizolowania systemu lub przerwania procesu przetwarzania. Celem jest zapewnienie ciągłości ochrony danych oraz niedopuszczenie do rozszerzenia się skutków nieprawidłowości.
- **Działania naprawcze** - podejmujemy kroki w celu przywrócenia stanu zgodnego z wysokimi standardami bezpieczeństwa i etyki. W przypadku incydentów o mniejszej skali, nasze działania skupiają się na pouczeniu i dodatkowym szkoleniu pracownika, co służy eliminacji nieświadomych błędów i podnoszeniu kompetencji cyfrowych. Przy zdarzeniach o większej złożoności, działania naprawcze obejmują korektę procesów merytorycznych, modyfikację parametrów narzędzi AI lub usuwanie niezasadnie wprowadzonych informacji z sesji roboczych, aby trwale wyeliminować przyczynę problemu.
- **Ocena skutków zdarzenia** - oceniamy zdarzenie pod kątem prawnym i merytorycznym, co pozwala na wyciągnięcie wniosków oraz aktualizację wewnętrznych wytycznych.

Typowe kategorie incydentów związanych z wykorzystaniem Systemów AI:

- **Wyciek danych** - wprowadzenie treści poufnych do narzędzia nieautoryzowanego, w szczególności danych krytycznych lub wrażliwych w rozumieniu Strategii AI.
- **Halucynacja** - przywołanie wygenerowanej przez AI analizy prawnej lub technicznej do oficjalnych dokumentów bez pełnej weryfikacji faktów/źródeł.

- **Stronniczość wprowadzana przez użytkownika** – wykorzystanie podatności modelu językowego na sugestię w celu przywołania wygenerowanej przez AI treści nieposiadającej przymiotu bezstronności do oficjalnych dokumentów.
- **Shadow AI** - korzystanie z prywatnych kont i nieautoryzowanych narzędzi AI do zadań służbowych.
- **Brak transparentności** - wykorzystanie AI do generowania treści publikacji urzędowych bez oznaczenia, że tekst został stworzony przy wsparciu sztucznej inteligencji.

7. Budowanie kompetencji AI

Nasi pracownicy posiadają niezbędne kompetencje AI, czyli adekwatny poziom wiedzy, umiejętności i świadomości w zakresie systemów AI, proporcjonalny do ich roli, odpowiedzialności oraz poziomu ryzyka związanego z wykorzystywanymi przez nich systemami AI[14].

Jako kompetencje AI rozumiemy:

- Zrozumienie podstawowych pojęć i zasad działania systemów AI.
- Świadomość ryzyk, ograniczeń i potencjalnych zagrożeń związanych ze stosowaniem systemów AI.
- Umiejętność bezpiecznego, odpowiedzialnego i zgodnego z prawem korzystania z systemów AI oraz ponoszenie pełnej odpowiedzialności za wykorzystanie wyników ich działania.
- Znajomość wymogów prawnych, w tym zasad ochrony informacji poufnych i danych osobowych;
- Zdolność identyfikacji sytuacji wymagających eskalacji do Zespołu ds. AI.
- Stosowanie Polityki AI[15].

Nasz system podnoszenia kompetencji opiera się na podejściu proporcjonalnym do poziomu wiedzy technicznej, doświadczenia i przeszkolenia pracownika, a także kontekstu wykorzystania przez niego systemów AI oraz wpływu wyników ich działania na osoby, których dotyczą[16]. Proces podnoszenia kompetencji rozpoczyna się przed rozpoczęciem pracy z systemami AI od zapoznania z aktualną Polityką AI i trwa nieprzerwanie w obrębie wykonywania obowiązków z wykorzystaniem narzędzi AI.

Dla osób korzystających z systemów AI w codziennej pracy uwzględniamy podnoszenie kompetencji w zakresie: praktycznego wykorzystania systemów AI, oceny wiarygodności wyników i ich interpretacji, roli człowieka w koncepcji human-in-the-loop oraz dokumentowania wykorzystania systemów AI. Rozwijamy również zespoły techniczne i wspierające systemy AI w ramach dedykowanych szkoleń, w szczególności z zakresu IT, data science i istotnych regulacji prawnych.

[14] art. 4 Rozporządzenia AI ACT
[15] art. 3 pkt 56 oraz motyw 20 preambuły Rozporządzenia AI ACT
[16] art. 4 Rozporządzenia AI ACT

8. Postanowienia końcowe

8.1. Wejście w życie

Polityka wchodzi w życie z dniem podpisania przez Prezesa Urzędu Patentowego RP.

Pracownicy Urzędu są zobowiązani do zapoznania się z treścią Polityki oraz poświadczenia tego faktu poprzez podpisanie oświadczenia pt. „Oświadczenie o zapoznaniu się z Polityką AI Urzędu Patentowego Rzeczypospolitej Polskiej". Podpisane oświadczenia pracowników przechowywane są w sekretariacie komórki organizacyjnej, w której pracownicy są zatrudnieni.

8.2. Przegląd i aktualizacja Polityki

Polityka podlega przeglądowi nie rzadziej niż raz w roku kalendarzowym. Przeglądu dokonuje Zespół ds. AI, uwzględniając w szczególności zmiany przepisów prawa, aktualne potrzeby Urzędu oraz wnioski płynące z dotychczasowego stosowania Polityki.

Zmiany Polityki wprowadza się w trybie właściwym dla jej przyjęcia.

8.3. Nadzór nad realizacją Polityki

Nadzór nad przestrzeganiem Polityki sprawuje Zespół ds. AI.

8.4. Współpraca przy realizacji Polityki

Zespół ds. AI współpracuje pełnomocnikiem ds. ochrony informacji niejawnych w zakresie ochrony informacji niejawnych, pełnomocnikiem ds. bezpieczeństwa cyberprzestrzeni w zakresie bezpieczeństwa cyberprzestrzeni i doradcą etycznym.

8.5. Zgłaszanie wątpliwości, uwag lub propozycji

Pracownik, który ma wątpliwości dotyczące stosowania Polityki, zauważy nieprawidłowości związane z wykorzystaniem AI, ma uwagi lub propozycje - powinien zgłosić sprawę bezpośredniemu przełożonemu lub Zespołowi ds. AI.

8.6. Dostępność Polityki

Polityka jest dokumentem jawnym. Jej treść udostępnia się w Biuletynie Informacji Publicznej Urzędu oraz w wewnętrznym systemie informacyjnym. Jawność Polityki realizuje zasadę przejrzystości działania administracji publicznej[17] oraz wspiera budowanie zaufania obywateli do sposobu wykorzystywania AI przez Urząd.

[17] art. 8 KPA

Załącznik nr 2 do zarządzenia nr 4
Prezesa Urzędu Patentowego RP
z dnia 18 maja 2026 r.

OŚWIADCZENIE

o zapoznaniu się z Polityką AI Urzędu Patentowego Rzeczypospolitej Polskiej

Ja niżej podpisany (a)

……. oświadczam, że:

1. Zapoznałem (am) się z Polityką AI Urzędu Patentowego Rzeczypospolitej Polskiej obowiązującą w Urzędzie Patentowym Rzeczypospolitej Polskiej.
2. Zobowiązuję się przestrzegać reguł i postanowień tej polityki w celu świadomego i odpowiedzialnego korzystania z narzędzi AI w swojej pracy.
3. Jestem świadomy, że moje działania w zakresie korzystania z narzędzi AI mogą być rejestrowane w celu zapewnienia bezpieczeństwa danych będących w posiadaniu Urzędu.
4. Jestem świadomy, że nieprzestrzeganie Polityki AI Urzędu Patentowego Rzeczypospolitej Polskiej może prowadzić do wyciągnięcia konsekwencji służbowych lub karnych.

…….. dnia ……..

/data i miejsce złożenia oświadczenia/

……..

/podpis osoby składającej oświadczenie/