Ministerstwo Cyfryzacji

Zakazane systemy AI

Spis treści

Materiał opracowany
przez ekspertów NASK

NASK

Wprowadzenie

Z początkiem sierpnia 2024 r. rozpoczął się w Unii Europejskiej proces wchodzenia w życie przepisów Rozporządzenia o sztucznej inteligencji[1] (dalej: Akt o AI, AI Act, Akt). Celem tych regulacji jest poprawa funkcjonowania rynku wewnętrznego UE przez zastosowanie jednolitych ram prawnych, w szczególności w zakresie rozwoju, wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów sztucznej inteligencji. Nowe przepisy mają pozwolić na zapewnienie bezpiecznego rozwoju godnej zaufania sztucznej inteligencji, która dzięki nim będzie wykorzystywana w Unii z poszanowaniem praw podstawowych. Jako że Akt nakłada obowiązki zarówno na osoby fizyczne, jak i prawne, jego przepisów będą musieli przestrzegać zarówno pracownicy sektora publicznego, jak i obywatele –oraz przedsiębiorcy.

Ważnym obowiązkiem, do przestrzegania którego przepisy Aktu zobowiązują już od 2 lutego 2025 r., jest zakaz używania oraz wprowadzania na rynek lub do obrotu systemów AI, które spełniają kryteria praktyk zakazanych. Oznacza to, że za używanie lub dystrybuowanie niektórych rodzajów programów i aplikacji wykorzystujących algorytmy sztucznej inteligencji nałożone mogą zostać dotkliwe administracyjne kary pieniężne. Ich maksymalna wysokość to 35 mln euro lub 7% całkowitego rocznego światowego obrotu z poprzedniego roku.

Szczegółowe informacje o charakterystyce i cechach systemów AI, które będą decydować o uznaniu ich za zakazane, opublikuje Komisja Europejska. Zanim jednak to nastąpi, konieczne jest podjęcie działań, które pozwolą przedsiębiorcom, urzędnikom czy obywatelom zrozumieć nowe przepisy oraz przygotować się na ich wejście w życie.

Celem publikacji jest wyjaśnienie przepisów Aktu dotyczących systemów sztucznej inteligencji objętych zakazem, a także przybliżenie technik, funkcji i sposobów ich działania. Dzięki lekturze będzie można uniknąć podejmowania działań, które zostaną ocenione jako naruszające przepisy art. 5 Aktu.

[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. (europa.eu).

Wejście w życie przepisów Aktu o AI

Akt o sztucznej inteligencji ustanawia jednolite obowiązki dla operatorów i gwarantuje spójną ochronę nadrzędnego interesu publicznego i praw osób na całym rynku wewnętrznym UE. Ma to zapobiegać rozbieżnościom, które utrudniają swobodny obrót systemami AI oraz powiązanymi produktami i usługami na rynku wewnętrznym, a także utrudniają innowacje w ich zakresie oraz ich wdrażanie i rozpowszechnianie. Akt nie zastępuje innych przepisów (takich jak np. RODO lub Akt o Usługach Cyfrowych), ale je uzupełnia.

Nowe prawo wprowadza zakaz stosowania niektórych praktyk w zakresie sztucznej inteligencji, określa wymogi dotyczące systemów AI wysokiego ryzyka i obowiązki spoczywające na operatorach oraz w zakresie przejrzystości w odniesieniu do niektórych systemów sztucznej inteligencji. Przepisy Aktu bazują na podejściu opartym na analizie ryzyka, dzięki czemu obowiązki będą proporcjonalne do skali ewentualnych zagrożeń.

Co do zasady, **przepisy Aktu będą obowiązywać po upływie 24 miesięcy od jego ogłoszenia,** jednak w przypadku części przepisów te terminy są zróżnicowane i wynoszą kolejno: 6, 12 i 36 miesięcy. **W lutym 2025 r. roku mocy nabiorą przepisy zakazujące stosowania w całej Unii szczególnie niebezpiecznych systemów AI** (zakazane praktyki określone w art. 5). Następnie, w sierpniu 2025 r. w życie wejdą przepisy kluczowe dla nadzoru nad sztuczną inteligencją dotyczące m.in. określenia organu nadzoru rynku i organu notyfikującego, modeli AI ogólnego przeznaczenia, jak również te dotyczące kar za naruszenia Aktu. Jako ostatnie zaczną obowiązywać przepisy, które odnoszą się do systemów AI wysokiego ryzyka oraz związanych z nimi obowiązków. Ich wejście w życie nastąpi w sierpniu 2025 r. oraz, w przypadku niektórych systemów wysokiego ryzyka będących elementem produktów podlegających osobnym normom, w sierpniu 2026 r.

Za opracowanie przepisów umożliwiających egzekwowanie Aktu w polskim systemie prawa odpowiada Ministerstwo Cyfryzacji. Wymaga to działań legislacyjnych, których rezultatem będzie przyjęcie ustawy umożliwiającej od 1 sierpnia 2025 r. nadzorowanie rynku sztucznej inteligencji w Polsce. Informacje na temat instytucji publicznych odpowiedzialnych za nadzór nad sektorem oraz o mechanizmach umożliwiających korzystanie z praw, które osobom fizycznym i prawnym przyznaje nowa regulacja, będą podawane do wiadomości za pośrednictwem strony internetowej Ministerstwa Cyfryzacji: (www.gov.pl/web/cyfryzacja).

Kto będzie podlegał nowym regulacjom i jaki jest zakres ich stosowania?

Akt o sztucznej inteligencji stosuje się do:

a. dostawców wprowadzających do obrotu lub oddających do użytku systemy AI lub wprowadzających do obrotu modele AI ogólnego przeznaczenia w Unii niezależnie od tego, czy dostawcy ci mają siedzibę lub znajdują się w Unii, czy w państwie trzecim,

b. podmiotów stosujących systemy AI, które mają siedzibę lub znajdują się w Unii,

c. dostawców systemów AI i podmiotów stosujących systemy AI, którzy mają siedzibę lub znajdują się w państwie trzecim, w przypadku gdy wyniki wytworzone przez system AI są wykorzystywane w Unii,

d. importerów i dystrybutorów systemów AI,

e. producentów produktu, którzy pod własną nazwą lub znakiem towarowym oraz wraz ze swoim produktem wprowadzają do obrotu lub oddają do użytku system AI,trzecim, w przypadku gdy wyniki wytworzone przez system AI są wykorzystywane w Unii,

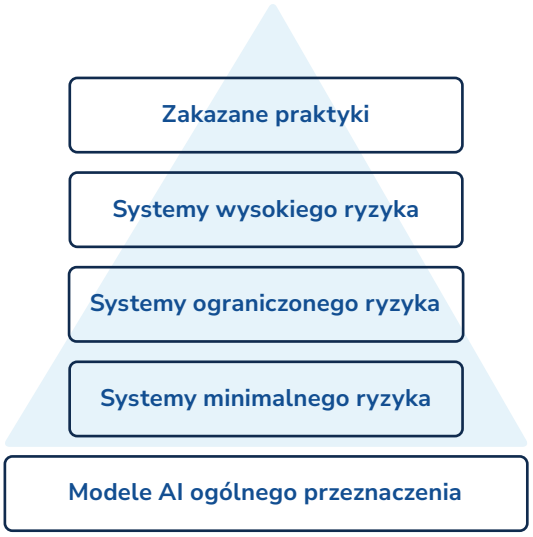
f. upoważnionych przedstawicieli dostawców niemających siedziby w Unii,

g. osób, na które AI ma wpływ i które znajdują się w Unii.

Co istotne, **Akt nie obejmuje modeli i systemów AI wykorzystywanych dla celów związanych z obronnością, bezpieczeństwem narodowym oraz badaniami i nauką.** Wyłączenie tej kategorii oznacza, że przy projektach badawczych nowe przepisy muszą być przestrzegane przez każdą osobę lub podmiot od momentu, gdy system lub model AI zostanie wprowadzony na rynek lub oddany do użytku, bez względu na to, czy jest to realizowane komercyjnie, czy bezpłatnie.

Kategorie ryzyka wprowadzane przez Akt o AI

Akt o sztucznej inteligencji klasyfikuje systemy AI w oparciu o analizę ryzyka, wprowadzając jego cztery główne kategorie:



Kategoria **zakazanych praktyk** jest potencjalnie najbardziej dotkliwą dla wszystkich podlegających przepisom Aktu o sztucznej inteligencji. Tym samym wymaga poświęcenia dodatkowego czasu oraz uwagi ze strony poszczególnych organów państwowych i odbiorców regulacji.

Czym są zakazane praktyki w zakresie AI?

Są to praktyki, których wykorzystanie wiąże się z nieakceptowalnym ryzykiem, czyli takie, których rezultaty mogą mieć wysoce nieetyczny lub niebezpiecznych charakter. Wynika to z szerszych wysiłków UE, mających na celu regulację sztucznej inteligencji w sposób minimalizujący ryzyko i chroniący obywateli przed potencjalnymi zagrożeniami związanymi z nowoczesnymi technologiami.

Co istotne, **Komisja Europejska zobowiązała się przedstawić przykłady systemów objętych zakazem** oraz podać szczegółowe informacje pozwalające ocenić, czy dany system wpisuje się w kryteria określone w Rozporządzeniu. Ma to nastąpić na przełomie 2024 i 2025 r. Do tego czasu jedynym źródłem informacji istotnych z punktu widzenia przestrzegania nowego prawa są przepisy Aktu o AI.

Zakazane praktyki w obszarze użycia systemów AI zostały wymienione w art. 5 Aktu i zalicza się do nich:

Stosowanie technik podprogowych, manipulacyjnych lub wprowadzających w błąd	skutkujących zniekształceniem podejmowanych przez daną osobę decyzji w sposób powodujący u niej lub innych osób istotne szkody
Wykorzystywanie słabości osoby fizycznej lub grupy osób	ze względu na ich wiek, niepełnosprawność lub szczególną sytuację społeczną lub ekonomiczną
	skutkujących zniekształceniem podejmowanych przez daną osobę decyzji, w sposób powodujący u niej lub innych osób istotne szkody
Scoring społeczny	tj. klasyfikacja osób fizycznych na podstawie ich zachowań społecznych lub cech osobistych
	jeśli prowadzi do krzywdzącego lub niekorzystnego traktowania
Profilowanie osoby fizycznej lub ocena jej cech osobowości	którego celem jest ocena ryzyka popełnienia przestępstwa
Tworzenie lub rozbudowywanie baz danych, służących rozpoznawaniu twarzy	służących rozpoznawaniu twarzy
	poprzez nieukierunkowane pozyskiwanie (untargeted scraping) wizerunków twarzy z internetu lub nagrań z telewizji przemysłowej
Wyciąganie wniosków na temat emocji osoby fizycznej	w miejscu pracy lub instytucjach edukacyjnych
Wykorzystywanie systemów kategoryzacji biometrycznej	które indywidualnie kategoryzują osoby fizyczne w oparciu o ich dane biometryczne
	by wydedukować lub wywnioskować informacje na temat ich rasy, poglądów politycznych, przynależności do związków zawodowych, przekonań religijnych lub światopoglądowych, seksualności lub orientacji seksualnej
Wykorzystywanie systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym	w przestrzeni publicznej do celów ścigania przestępstw

Tabela 1. Zakazane praktyki w obszarze użycia systemów AI, oprac. własne na podstawie art. 5 AIA

Praktyki zakazane na gruncie Aktu o AI

Techniki podprogowe, manipulacyjne i wprowadzające w błąd

Zakaz ten dotyczy wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów sztucznej inteligencji, których celem jest manipulacja zachowaniem osoby lub grupy osób, skutkująca lub mogąca skutkować wyrządzeniem poważnej szkody. Jednak aby uznać, że wykorzystanie takich systemów jest niedopuszczalne, muszą zostać spełnione określone warunki.

Zakazane są systemy AI, które stosują **techniki podprogowe,** będące poza świadomością danej osoby lub celowe **techniki manipulacyjne lub wprowadzające w błąd**. Wobec tego, aby stwierdzić, czy system kwalifikuje się pod ten zakaz, w pierwszej kolejności konieczne jest zweryfikowanie, czy wykorzystuje on którąś z nich. Warto przy tym zauważyć, że w przypadku technik manipulacyjnych i wprowadzających w błąd przepis stanowi, że ich stosowanie musi być celowe – co oznacza, że stoi za nim intencja podmiotu lub osoby, która system AI wprowadza do obrotu, oddaje do użytku lub wykorzystuje.

Skutkiem lub celem zastosowania technik podprogowych, manipulacyjnych lub wprowadzających w błąd jest dokonanie **znaczącej zmiany zachowania** danej osoby lub grupy osób poprzez ograniczenie ich zdolności do podejmowania świadomych decyzji – przykładowo wywołując sytuację, w której działanie nie zostałoby podjęte, gdyby nie zastosowano wspomnianych technik. Jednocześnie taka sztucznie wywołana decyzja wyrządza lub może wyrządzać poważną szkodę u osoby lub grupy.

Należy podkreślić, że podział zarówno na „skutek", jak i „cel" oznacza, że system nie musi faktycznie wywołać znaczącej zmiany zachowania i poważnej szkody – wystarczy, że wykazane zostanie, że miało to stanowić rezultat jego działania.

System AI może zostać uznany za zakazany jako stosujący **techniki podprogowe,** będące poza świadomością danej osoby lub celowe **techniki manipulacyjne czy wprowadzające w błąd**, jeśli łącznie wystąpią następujące okoliczności:

zastosowanie przez system AI technik podprogowych, manipulacyjnych lub wprowadzających w błąd;

Przykład

Za przykład w tej kategorii może posłużyć- system AI wdrażany jako narzędzie marketingowe w centrach handlowych, którego głównym celem jest subtelne wpływanie na decyzje zakupowe klientów, aby zwiększyć sprzedaż określonych produktów.

System wykorzystuje techniki podprogowe poprzez delikatne dźwięki i obrazy emitowane w ramach reklam w centrum handlowym. Na przykład, podczas słuchania muzyki w sklepie, klient może nieświadomie usłyszeć słowa takie jak „kup", „potrzebujesz" czy „teraz", co skłania go do zakupu.

System może również manipulować reklamami wyświetlanymi na ekranach w centrum handlowym. Analizuje dane o klientach, takie jak ich nawyki zakupowe, historie transakcji oraz dane z mediów społecznościowych, prezentując w reklamach produkty w taki sposób, aby wywołać u klienta wrażenie, że są one niezbędne lub specjalnie dostosowane do jego potrzeb, mimo że tak nie jest.

skutek lub cel w postaci zmiany zachowania, w ramach której dochodzi do:

- znaczącego ograniczenia zdolności do podejmowania świadomych decyzji u osoby lub grupy osób,
- podjęcia przez osobę lub grupę osób decyzji, której inaczej by nie podjęły,
- podjęcia decyzji w sposób, który wyrządza lub może wyrządzić u danej osoby, innej osoby lub grupy osób poważną szkodę.

Przykład

Przykładem może być system AI, który jest reklamowany jako narzędzie wspierające osoby starsze i niepełnosprawne w zarządzaniu ich finansami oraz codziennymi decyzjami zakupowymi, który jednocześnie wykorzystuje gromadzone dane do wywierania na użytkownikach presji w celu podjęcia przez nich zobowiązań finansowych. System jest promowany jako asystent osobisty, który pomaga w podejmowaniu najlepszych decyzji finansowych, zapewniając poczucie bezpieczeństwa i komfortu. Wykorzystuje zaawansowane techniki manipulacyjne, aby skłonić użytkowników np. do zakupu produktów finansowych, które nie są dla nich korzystne, takich jak wysoko oprocentowane pożyczki czy kosztowne polisy ubezpieczeniowe. Jako system przeznaczony dla osób starszych oraz z niepełnosprawnościami wykorzystuje ich ograniczoną zdolność do samodzielnego podejmowania decyzji finansowych.

Wykorzystywanie słabości osoby lub grupy osób

Szczególną ochroną objęte są także osoby szczególnie wrażliwe, które ze względu na wiek, niepełnosprawność lub sytuację społeczną czy ekonomiczną mogą być wyjątkowo narażone na manipulację. Są to na przykład osoby mające długotrwale naruszoną sprawność fizyczną, psychiczną, intelektualną lub w zakresie zmysłów, żyjące w skrajnym ubóstwie, z mniejszości etnicznych lub religijnych.

Z tego powodu zakazuje się stosowania systemów AI, które wykorzystywałyby wyżej wskazane słabości, czego celem lub skutkiem byłoby dokonanie znaczącej zmiany zachowania w sposób, który wyrządza lub może z uzasadnionym prawdopodobieństwem wyrządzić poważną szkodę.

System AI może zostać uznany za zakazany jako wykorzystujący słabości szczególnie wrażliwych osób lub grup, jeśli łącznie wystąpią następujące okoliczności:

- wykorzystanie przez system AI słabości osoby lub grupy osób ze względu na wiek, niepełnosprawność lub szczególną sytuację społeczną czy ekonomiczną,
- skutek lub cel w postaci dokonania znaczącej zmiany zachowania w sposób, który wyrządza lub może z uzasadnionym prawdopodobieństwem wyrządzić u tej lub u innej osoby poważną szkodę.

Przykład

Przykładem w tym zakresie może być system AI wdrażany przez władze miejskie w celu monitorowania i oceny zachowań mieszkańców w wielu aspektach ich życia. Jego celem jest promowanie „dobrych" zachowań społecznych poprzez przyznawanie punktów za pozytywne działania oraz odejmowanie za negatywne.

System zbiera dane z różnych źródeł, takich jak kamery monitoringu, media społecznościowe, aplikacje mobilne, a nawet systemy płatności. Na podstawie tych danych ocenia zachowanie mieszkańców, takie jak ich aktywność w lokalnych społecznościach, nawyki zakupowe, interakcje z innymi osobami, a nawet przestrzeganie przepisów drogowych. System przyznaje punkty za działania uznane za pozytywne, np. uczestnictwo w lokalnych wydarzeniach, wolontariat, segregowanie odpadów, a odejmuje za zachowania uznane za negatywne, np. łamanie przepisów, otrzymywanie mandatów, negatywne komentarze w mediach społecznościowych.

Mieszkańcy z niskim wynikiem mogą doświadczać różnorodnych niekorzystnych skutków, jak trudności w znalezieniu pracy, problem z wynajmem mieszkań, wyższe opłaty za usługi publiczne, a nawet ograniczenia w dostępie do niektórych usług miejskich. System może także prowadzić do nieproporcjonalnego traktowania osób. Na przykład pojedyncze, mało istotne zdarzenie, takie jak spóźnienie się na określone spotkanie, może prowadzić do znacznego obniżenia punktów i związanego z tym wykluczenia z istotnych aspektów życia społecznego.

Scoring społeczny

Ta kategoria obejmuje zakaz wprowadzania do obrotu, oddawania do użytku lub wykorzystywania **systemów AI na potrzeby oceny lub klasyfikacji osób fizycznych lub grup osób,** prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych, wywnioskowanych lub przewidywanych cech osobistych lub osobowości, **kiedy to scoring społeczny prowadzi do określonych skutków.** Należą do nich:

- krzywdzące lub niekorzystne traktowanie, **które nie jest związane z kontekstami, w których pierwotnie wygenerowano lub zebrano dane,**
- krzywdzące lub niekorzystne traktowanie niektórych osób fizycznych lub ich grup, **nieuzasadnione lub nieproporcjonalne do ich zachowania** społecznego lub jego wagi.

Oznacza to, że zakazane jest wykorzystywanie systemów AI, które mają oceniać lub klasyfikować osobę lub grupę osób przez pryzmat określonego zachowania, cechy osobistej lub osobowości. Przy czym należy podkreślić, że wykorzystywanie systemów scoringu społecznego jest zakazane tylko wtedy, gdy prowadzi do określonych, niekorzystnych skutków w odniesieniu do ocenianych osób. W praktyce oznacza to, że ten zakaz nie powinien mieć wpływu na zgodne z prawem praktyki oceny osób fizycznych, takich jak np. ocena zdolności kredytowej na podstawie historii kredytowania czy dotychczasowych spłat zobowiązań finansowych.

Kategoryzacja biometryczna

Zakazane jest także wykorzystywanie systemów kategoryzacji biometrycznej, które indywidualnie kategoryzują osoby fizyczne w oparciu o ich dane biometryczne[2], **by wydedukować lub wywnioskować informacje na temat ich rasy, poglądów politycznych, przynależności do związków zawodowych, przekonań religijnych lub światopoglądowych, seksualności lub orientacji seksualnej.**

W akcie o sztucznej inteligencji zakaz stosowania systemów kategoryzacji biometrycznej jest ogólny, nie dotyczy wyłącznie konkretnej kategorii technik biometrycznych, czyli obejmuje obie – silne (twarde) i słabe (miękkie). W rozporządzeniu wskazano, że pojęcie „kategoryzacji biometrycznej" to **przypisywanie osób fizycznych do określonych kategorii na podstawie danych biometrycznych.**

[2]Rozporządzenie o sztucznej inteligencji definiuje dane biometryczne w ten sam sposób, co ogólne rozporządzenie o danych osobowych. Termin ten oznacza dane osobowe będące wynikiem specjalnego przetwarzania technicznego, które dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej, takich jak wizerunek twarzy lub dane daktyloskopijne. Powszechnie wyróżnia się dwa rodzaje technik biometrycznych: silne (twarde) i słabe (miękkie). Do pierwszej grupy zalicza się identyfikatory, które umożliwiają lub potwierdzają unikalną identyfikację osoby fizycznej, np. odciski palców czy tęczówka lub siatkówka oka. Z kolei drugą grupę stanowią cechy, które są „mniej unikalne" lub „mniej stabilne", np. podpis, kształt ucha lub twarzy, wzorce zachowań, głos czy sposób chodu. Miękkie dane biometryczne obejmują cechy, które mają charakter ogólny i nie są jednoznacznie kojarzone z daną osobą, np. płeć lub wiek.

Mogą to być takie aspekty jak płeć, wiek, kolor włosów, kolor oczu, tatuaże, cechy behawioralne bądź osobowości, język, religia, przynależność do mniejszości narodowej, orientacja seksualna lub poglądy polityczne.

Wyjątkiem od zakazu stosowania systemów kategoryzacji biometrycznej są dwa przypadki:

- etykietowanie lub filtrowanie pozyskanych zgodnie z prawem zbiorów danych biometrycznych, takich jak obrazy, w oparciu o dane biometryczne,
- kategoryzacja danych biometrycznych **w obszarze ścigania przestępstw.**

Dopuszczalny będzie proces, w którym dane biometryczne są analizowane i przypisywane do odpowiednich kategorii lub oznaczeń (etykiet). Przykładowo obrazy twarzy mogą być etykietowane według emocji, wieku, płci itp., co jest kluczowym procesem dla trenowania i doskonalenia algorytmów sztucznej inteligencji. **Nie będzie zakazane również wykorzystywanie systemów AI** do filtrowania pozyskanych zgodnie z prawem zbiorów danych biometrycznych, czyli **do selekcji i wyodrębniania określonych danych biometrycznych z większego zbioru** na podstawie wybranych kryteriów. Celem filtrowania jest uzyskanie odpowiednich podzbiorów danych, które są istotne dla określonego zastosowania lub analizy.

Dopuszcza się także wykorzystywanie systemów kategoryzacji biometrycznej w obszarze ścigania przestępstw. Oznacza to, że **tego rodzaju technologie mogą być używane przez organy ścigania** lub w ich imieniu **w celu zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub wykonywania kar,** w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania im. Zgodne z Rozporządzeniem wykorzystanie takich systemów dla powyższych celów podlegać będzie przepisom przewidzianym dla systemów wysokiego ryzyka.

Zakaz nie obejmuje także systemów kategoryzacji biometrycznej, które pełnią jedynie funkcję pomocniczą, nieodłącznie związaną z inną usługą komercyjną. Oznacza to, że z obiektywnych względów technicznych funkcja ta nie może być wykorzystywana bez usługi głównej. **Przykładem takiego dopuszczalnego użycia kategoryzacji biometrycznej** mogą być filtry klasyfikujące cechy twarzy lub ciała, wykorzystywane na internetowych platformach handlowych. Główną

Przykład

Za przykład może posłużyć tutaj system AI wykorzystywany np. przez dużą korporację do analizy danych biometrycznych swoich pracowników oraz kandydatów do pracy. Jego celem jest rzekome zwiększenie efektywności zarządzania zasobami ludzkimi poprzez „lepsze dopasowanie" pracowników do odpowiednich stanowisk na podstawie ich danych biometrycznych.

System zbiera z kamer monitoringu, urządzeń biometrycznych w miejscu pracy oraz aplikacji mobilnych używanych przez pracowników szerokie spektrum danych biometrycznych, w tym skany twarzy, odciski palców, analizę głosu, a nawet informacje o posturze i sposobie poruszania się. Na podstawie tych danych kategoryzuje pracowników według różnych cech osobistych i osobowościowych. Na podstawie mimiki twarzy i analizy głosu system może wywnioskować poglądy polityczne pracownika lub jego przekonania religijne. Podobnie analiza zachowań i interakcji w miejscu pracy może prowadzić do wniosków na temat przynależności do związków zawodowych czy orientacji seksualnej.

Na podstawie uzyskanych informacji pracownicy są kategoryzowani i traktowani w zróżnicowany sposób. Pracownicy o pewnych cechach mogą być dyskryminowani, np. nie dostawać awansów, być pomijani przy podwyżkach lub przenoszeni na mniej korzystne stanowiska. Osoby o określonych poglądach politycznych lub przynależności do związków zawodowych mogą być celowo wykluczane z ważnych projektów lub zwalniane pod pretekstem „niedopasowania".

usługą w tym przypadku będzie sprzedaż produktu, a funkcją pomocniczą – umożliwienie konsumentowi uzyskania wyobrażenia, jak produkt będzie się na nim prezentował, aby pomóc mu w podjęciu decyzji o zakupie. Drugim przykładem mogą być filtry stosowane w internetowych serwisach społecznościowych, które kategoryzują cechy twarzy lub ciała, aby umożliwić użytkownikom dodawanie lub modyfikowanie zdjęć lub filmów wideo. Filtry takie nie mogą być stosowane bez usługi głównej, która polega na udostępnianiu treści online w ramach serwisu społecznościowego.

Zakazem objęte są **wyłącznie** systemy kategoryzacji biometrycznej, których celem jest **wydedukowanie lub wywnioskowanie na podstawie danych biometrycznych konkretnej osoby informacji na temat jej:**

- **rasy,**
- **poglądów politycznych,**
- **przynależności do związków zawodowych,**
- **przekonań religijnych lub światopoglądowych,**
- **seksualności lub orientacji seksualnej.**

Niezależnie od tego zakazu, szczególną ochroną otoczone są także systemy AI przeznaczone do kategoryzacji biometrycznej na podstawie danych biometrycznych według wrażliwych atrybutów lub cech chronionych na podstawie RODO. Do tej kategorii zalicza się dane osobowe, ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne. Systemy kategoryzacji biometrycznej tego rodzaju klasyfikowane są jako systemy wysokiego ryzyka i spełniać muszą określone w AI Act wymogi.

Ocena lub przewidywanie ryzyka popełnienia przestępstwa

Rozporządzenie o sztucznej inteligencji zakazuje **wprowadzania do obrotu, oddawania do użytku w tym konkretnym celu** lub **wykorzystywania systemów AI do oceny lub przewidywania ryzyka popełnienia przestępstwa przez osobę fizyczną wyłącznie na podstawie profilowania lub oceny cech osobowości i cech charakterystycznych.**

Profilowanie odnosi się do automatycznego przetwarzania danych osobowych w celu oceny pewnych aspektów dotyczących osoby fizycznej, takich jak jej zachowanie, cechy osobowości

Przykład

W tej kategorii przykładem może być system opracowany przez firmę zajmującą się technologią bezpieczeństwa i oferowany instytucjom takim jak szkoły, firmy ochroniarskie czy organy ścigania, którego celem jest przewidywanie ryzyka popełnienia przestępstwa przez osoby fizyczne na podstawie analizy ich cech osobowościowych i charakterystycznych.

System zbiera dane z różnych źródeł, takich jak media społecznościowe, rejestry publiczne, repozytoria danych demograficznych, a nawet baz wyników psychologicznych testów online. Na podstawie tych danych system analizuje cechy osobowościowe i psychologiczne, takie jak impulsywność, skłonność do agresji, poziom empatii i inne. Następnie algorytmy przetwarzają zebrane dane i tworzą profil ryzyka dla każdej osoby.

System automatycznie klasyfikuje osoby jako „niskiego", „średniego" lub „wysokiego" ryzyka popełnienia przestępstwa. Na przykład osoba, która często wyraża negatywne emocje w mediach społecznościowych i ma historię drobnych wykroczeń, może zostać oznaczona jako „wysokiego ryzyka".

Może ona doświadczać dyskryminacji, np. mieć trudności w znalezieniu pracy, być obiektem zwiększonej inwigilacji przez służby bezpieczeństwa lub nawet być profilaktycznie zatrzymywana przez policję.

czy charakterystyka. Ocena cech osobowości i cech charakterystycznych obejmuje analizę takich aspektów, jak cechy psychologiczne, zachowania, preferencje itp. Przykładem systemu AI potencjalnie zakazanego na gruncie Rozporządzenia o sztucznej inteligencji może być system, opierający się **wyłącznie** na analizie cech osobowości i wcześniejszych zachowań – przykładowo analizujący dane z mediów społecznościowych, historię przestępstw, dane demograficzne i inne informacje osobiste, aby stworzyć profil ryzyka. Zgodnie z przepisami taki system byłby zakazany, chyba że jego wyniki byłyby jedynie **wsparciem dla oceny dokonywanej przez człowieka**, która opierałaby się na obiektywnych i weryfikowalnych faktach związanych z działalnością przestępczą.

Wyjątki od zakazu stosowania systemów AI do oceny lub przewidywania ryzyka przestępczości są ściśle określone i mają na celu zapewnienie, że takie systemy są używane w sposób odpowiedzialny i zgodny z prawami człowieka. Systemy do oceny lub przewidywania ryzyka popełnienia przestępstwa mogą być wykorzystywane do **wspierania oceny dokonywanej przez człowieka,** pod warunkiem że ocena ta opiera się na **obiektywnych i weryfikowalnych faktach bezpośrednio związanych z działalnością przestępczą.**

Systemy tego typu będą mogły analizować cechy osobowości i wcześniejsze zachowania pod warunkiem, że ostateczną decyzję na podstawie przeanalizowanych i sformułowanych przez program materiałów podejmie człowiek – operator, analityk lub osoba o innej roli. Formułowana ocena powinna opierać się na faktach o konkretnej charakterystyce, które muszą być:

1. obiektywne,
2. weryfikowalne,
3. bezpośrednio związane z działalnością przestępczą.

Obiektywność faktów bezpośrednio związanych z działalnością przestępczą powinna zakładać niedyskryminacyjne gromadzenie materiałów lub informacji (zarówno na korzyść, jak i obciążających obiekt oceny) w toku oceny dokonywanej przez człowieka i wspieranej systemami do oceny lub przewidywania ryzyka popełnienia przestępstwa. Z kolei informacje są sprawdzalne, **jeśli można potwierdzić je same albo dane wejściowe wykorzystane do ich uzyskania, a także jeśli różni, dysponujący odpowiednią wiedzą i niezależni**

obserwatorzy mogliby dojść do konsensusu, ale już niekoniecznie do pełnej zgody, że **konkretne przedstawienie stanowi wierne odzwierciedlenie rzeczywistości.** Sprawdzalność pozwala uzyskać pewność, że informacje są **kompletne, neutralne i dokładne.** Dodatkowo, innym sposobem zwiększającym sprawdzalność informacji jest **przekazanie tych poddanych przeglądowi i uzgodnionych przez organy administrujące, zarządzające i nadzorcze lub ich komitety.**

Zdalna identyfikacja biometryczna w czasie rzeczywistym w przestrzeni publicznej do celów ścigania przestępstw

Na gruncie AI Act państwa mogą wprowadzić przepisy umożliwiające pełne lub częściowe zezwolenie na wykorzystanie **systemów AI jako systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów ścigania przestępstw.** Zasadniczym warunkiem ich wykorzystania jest to, aby było to **bezwzględnie konieczne** do osiągnięcia jednego z trzech enumeratywnie wyliczonych w regulacji celów:

a. ukierunkowanego poszukiwania osób zaginionych lub ofiar takich czynów jak uprowadzenia, handel ludźmi lub wykorzystywania seksualnego,

b. zapobiegnięcia konkretnemu, istotnemu i bezpośredniemu zagrożeniu życia, bezpieczeństwa fizycznego osób lub rzeczywistemu i aktualnemu lub dającemu się przewidzieć zagrożeniu atakiem terrorystycznym,

c. lokalizowania lub identyfikowania osoby podejrzanej o popełnienie przestępstwa w celu prowadzenia postępowania przygotowawczego, ścigania lub wykonania kar w odniesieniu do przestępstw wyraźnie wskazanych w załączniku II do Rozporządzenia o sztucznej inteligencji i podlegających w danym państwie członkowskim karze pozbawienia wolności lub środkowi polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej cztery lata.

Dodatkowo systemy tego typu mogą być wykorzystywane jedynie w celu **potwierdzenia tożsamości konkretnej poszukiwanej osoby,** przy czym konieczne jest także uwzględnienie określonych elementów:

Przykład

W tym zakresie przykładem może być system AI mający na celu zdalną identyfikację biometryczną w czasie rzeczywistym w przestrzeni publicznej, wykorzystywany przez lokalne służby porządkowe w ramach standardowych działań operacyjnych. System taki wykorzystuje sieć kamer monitoringu, wyposażonych w technologię rozpoznawania twarzy. Następnie przesyłane do centralnej bazy dane są analizowane i porównywane z bazą danych osób podejrzanych o popełnienie przestępstw. Rozwiązanie działa w sposób ciągły, monitorując wszystkich ludzi w przestrzeni publicznej bez ich wiedzy i zgody. Władze miejskie decydują się na jego użycie, aby ścigać drobne przestępstwa, takie jak kradzieże kieszonkowe i graffiti. Taki system nie spełniałby wymogów prawnych (konieczności, proporcjonalności i ochrony praw obywatelskich) oraz prowadziłby do inwazyjnej inwigilacji, naruszenia prywatności oraz potencjalnie niesprawiedliwego traktowania obywateli na podstawie niezweryfikowanych i niepełnych danych biometrycznych.

a. charakteru sytuacji, w szczególności jej powagę, a także prawdopodobieństwo i skalę szkody, która powstałaby, jeżeli nie wykorzystano by systemu,

b. konsekwencji wykorzystania systemu dla praw i wolności, w szczególności ich powagi, prawdopodobieństwa i skali.

Ponadto, należy także wziąć pod uwagę, iż wykorzystanie takich systemów musi przebiegać z zachowaniem **niezbędnych i proporcjonalnych zabezpieczeń oraz warunków,** w tym w szczególności w zakresie ograniczeń czasowych, geograficznych i osobowych.

Możliwość wykorzystania systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej przez organy ścigania zależy od przeprowadzenia **oceny jego skutków w zakresie praw podstawowych**[3]. To ta sama procedura, która jest przeznaczona dla systemów AI wysokiego ryzyka. **Musi ona obejmować:**

a. **opis procesów podmiotu stosującego,** w których system będzie wykorzystywany zgodnie z jego przeznaczeniem,

b. **opis okresu,** w którym każdy systemAI ma być wykorzystywany, i opis częstotliwości tego wykorzystywania,

c. **kategorie osób fizycznych i grup,** na które może mieć wpływ wykorzystywanie systemu,

d. **opis szczególnego ryzyka szkody,** które może mieć wpływ na kategorie osób fizycznych lub grupy osób zidentyfikowanych zgodnie z poprzednim punktem, z uwzględnieniem informacji przekazanych przez dostawcę systemu AI, zgodnie z zaleceniem przejrzystości i udostępniania informacji podmiotom stosującym, w tym instrukcji obsługi,

e. **opis wdrożenia środków nadzoru ze strony człowieka,** zgodnie z instrukcją obsługi,

f. **środki,** jakie należy podjąć w przypadku urzeczywistnienia się ryzyka, w tym ustalenia dotyczące **zarządzania wewnętrznego i mechanizmów rozpatrywania skarg.**

Dodatkowo konieczne jest z**arejestrowanie systemu w unijnej bazie danych dla systemów wysokiego ryzyka.** Możliwe jest jednakże rozpoczęcie korzystania z systemów zdalnej identyfikacji biometrycznej w **należycie uzasadnionych, nadzwyczajnych** przypadkach bez rejestracji w bazie danych, aczkolwiek musi ona zostać dokonana bez zbędnej zwłoki.

[3]Prawa podstawowe w UE są chronione na mocy Karty praw podstawowych UE i należą do nich: prawo do godności człowieka, prawo do poszanowanie życia prywatnego i rodzinnego, ochrona danych osobowych, wolność wypowiedzi i informacji, wolność zgromadzania się i stowarzyszania się, prawo do niedyskryminacji, prawo do edukacji, ochrona konsumentów, prawa pracownicze, prawa osób z niepełnosprawnościami, równość płci, prawa własności intelektualnej, prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu, prawo do obrony i domniemania niewinności, prawo do dobrej administracji.

Każde użycie systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów ścigania przestępstw wymaga uprzedniego zezwolenia. Zezwolenie to musi być udzielone przez **organ wymiaru sprawiedliwości** lub **niezależny organ administracyjny** państwa członkowskiego, w którym ma nastąpić wykorzystanie systemu. Jest wydawane na uzasadniony wniosek i zgodnie ze szczegółowymi przepisami prawa krajowego. Organ musi także wziąć pod uwagę charakter sytuacji i konsekwencje wykorzystania takiego systemu dla praw i wolności wszystkich zainteresowanych osób. Zezwolenie jest udzielane na uzasadniony wniosek i zgodnie ze szczegółowymi przepisami prawa krajowego, na podstawie obiektywnych dowodów lub jasnych przesłanek na to, że wykorzystanie systemu jest konieczne i proporcjonalne do osiągnięcia określonych celów. Organ wydający zezwolenie musi także wziąć pod uwagę charakter sytuacji i konsekwencje wykorzystania takiego systemu dla praw i wolności wszystkich zainteresowanych osób.

Każde użycie systemu zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów ścigania przestępstw **musi być** zgłoszone **właściwemu organowi nadzoru rynku i krajowemu organowi ochrony danych** zgodnie z krajowymi przepisami prawa w zakresie wniosków o zezwolenie, ich wydawania, wykonywania oraz nadzoru nad tymi działaniami. Powiadomienie to nie może jednak zawierać wrażliwych danych operacyjnych.

Przykład

Przykładem w tej kategorii może być system AI rozwijany przez firmę technologii rozpoznawania twarzy, który automatycznie przeszukuje internet, w tym media społecznościowe, strony internetowe, fora dyskusyjne i inne źródła publicznie dostępnych zdjęć prawdziwych osób. Zgodnie z intencją twórców, ma on skanować każdą stronę i pobierać zdjęcia twarzy, bez wiedzy i zgody osób, których wizerunki są pozyskiwane. System jest również zintegrowany z systemami telewizji przemysłowej (CCTV) w różnych miastach. Dane pozyskane z tych źródeł są następnie automatycznie analizowane, a wizerunki twarzy są wyodrębniane i dodawane do bazy danych.

Na użycie takiej bazy danych decyduje się firma XYZ, która zarządza popularnym serwisem społecznościowym. System ma służyć do analizy użytkowników i dostarczania spersonalizowanych reklam. Zebrane dane są wykorzystywane do tworzenia szczegółowych profili behawioralnych, które są następnie sprzedawane firmom reklamowym. Użytkownicy zaczynają otrzymywać inwazyjne i spersonalizowane reklamy, które budzą ich niepokój i poczucie naruszenia prywatności.

Scraping

Kolejną zakazaną w akcie o sztucznej inteligencji praktyką jest tzw. scraping. Niedozwolone jest wprowadzanie do obrotu, oddawanie do użytku w tym konkretnym celu lub wykorzystywanie systemów AI, które **tworzą lub rozbudowują bazy danych służące rozpoznawaniu twarzy poprzez niecelowane pozyskiwanie (ang. scraping) wizerunków twarzy z internetu lub nagrań z telewizji przemysłowej.**

Scraping (ang. web scraping) to proces najczęściej automatycznego pozyskiwania dużej ilości danych z witryn internetowych, w tym wizerunku twarzy lub nagrań z telewizji przemysłowej. Dane pozyskane w ten sposób mogą być wykorzystywane na przykład do analizy rynku, prowadzenia badań naukowych, monitorowania opinii na temat poszczególnych produktów i usług, a także do trenowania generatywnych modeli sztucznej inteligencji. Mimo

że scraping jest uważany za efektywną metodę pozyskiwania danych z wielu źródeł, to budzi wiele wątpliwości w zakresie etyki i legalności.

Przykład

W tej kategorii przykładem może być system rozwijany przez firmę zajmującą się technologiami HR i oferowany firmom jako narzędzie do monitorowania emocji pracowników w miejscu pracy. Ma on na celu poprawę efektywności i dobrostanu pracowników poprzez analizę ich emocji w czasie rzeczywistym. Wykorzystuje kamery i mikrofony zamontowane w biurach, salach konferencyjnych i innych miejscach pracy, rejestruje wyrazy twarzy, ton głosu, gesty oraz inne wskaźniki emocji pracowników podczas ich codziennych aktywności. Algorytmy AI analizują zebrane dane w czasie rzeczywistym, wyciągając wnioski na temat emocji pracowników, takich jak stres, zadowolenie, frustracja czy zaangażowanie. Następnie system tworzy raporty i profile emocjonalne dla każdego pracownika. Pracownicy nie są w pełni świadomi, że ich emocje są monitorowane i analizowane. Menedżerowie wykorzystują stworzone przez system raporty do podejmowania decyzji personalnych. Pracownicy, którzy wykazują emocje takie jak stres czy frustracja, są oznaczani jako mniej produktywni, co prowadzi do niesprawiedliwych ocen wydajności i pomijania przy awansach.

Rozpoznawanie emocji

Kolejną zakazaną w akcie o sztucznej inteligencji praktyką jest tzw. system rozpoznawania emocji. Zakazane jest **wykorzystywanie systemów AI do wyciągania wniosków na temat emocji osoby fizycznej w miejscu pracy lub instytucjach edukacyjnych, z wyjątkiem przypadków, w których system AI ma zostać wdrożony lub wprowadzony do obrotu ze względów medycznych lub bezpieczeństwa;**

Systemy AI **wykorzystywane do wyciągania wniosków na temat emocji osoby fizycznej w miejscu pracy lub instytucjach edukacyjnych** mogą mieć szerokie zastosowanie w wielu sektorach, takich jak:

- HR i rekrutacje – analiza emocji podczas procesu rekrutacji w celu oceny zachowań kandydatów, ich reakcji podczas rozmów kwalifikacyjnych,
- instytucje edukacyjne i badawcze – analiza emocji podczas badań i eksperymentów,
- agencje marketingowe – analiza emocji w celu oceny skuteczności kampanii reklamowych,
- przedsiębiorstwa z sektora technologicznego – analiza emocji podczas opracowania nowych rozwiązań i ich implementacji,
- służby – analiza emocji podczas przesłuchań, rozmów, badań ewaluacyjnych.

Jak zapewnić zgodność wykorzystywanych systemów AI?

Prace nad zapewnieniem zgodności należy rozpocząć od przygotowania listy wykorzystywanych systemów AI.

Następnie należy przyporządkować wykorzystywane systemy AI na podstawie celu, funkcjonalności i rodzaju przetwarzanych danych

W dalszej kolejności należy dokonać oceny wykorzystywanych systemów AI i ustalenia, czy którykolwiek system AI należy do zakazanych kategorii.

Szczególną trzeba zwrócić uwagę na systemy wykorzystywane do prowadzenia interakcji z klientem, podejmowania decyzji oraz przetwarzających dane wrażliwe, także biometryczne,

W przypadku zidentyfikowania systemu AI jako potencjalnie zabronionego warto przygotować plan zaprzestania stosowania takiego systemu lub plan modyfikacji w celu zapewnienia zgodności.

Warto również rozważyć opracowanie wewnętrznych polityk i procedur monitorowania systemów AI w celu zapobiegania niezgodności.

Należy także zapewnić warunki do prowadzenia ewidencji wykorzystywanych systemów AI, a także przeprowadzonych ocen i podjętych środków zgodności.

Należy pamiętać, że **art. 50 Rozporządzenia o sztucznej inteligencji** zawiera szereg wymogów w zakresie transparentności systemów AI oraz określa obowiązki w zakresie przejrzystości dla dostawców i użytkowników niektórych systemów. **Podmioty stosujące dopuszczalne systemy kategoryzacji biometrycznej i rozpoznawania emocji do celów wykrywania przestępstw, przeciwdziałania im oraz prowadzenia postępowań przygotowawczych w związku z przestępstwami mają obowiązek informowania osób fizycznych,** wobec których systemy te są stosowane, **o fakcie ich wykorzystania.** Obowiązek ten nie ma zastosowania do systemów AI, których wykorzystywanie jest dozwolone z mocy prawa do wspomnianych celów.

W przypadku systemów AI przeznaczonych do wchodzenia w bezpośrednią interakcję z osobami fizycznymi mają one być projektowane i rozwijane w taki sposób, aby zainteresowane osoby fizyczne były o tym informowane. Wyjątkiem jest sytuacja, kiedy jest to oczywiste dla dostatecznie poinformowanej, uważnej i ostrożnej osoby fizycznej, z uwzględnieniem okoliczności i kontekstu wykorzystywania systemu AI. Jest to więc dodatkowe zabezpieczenie przed podejmowaniem decyzji lub działań, które mogłyby wynikać z braku świadomości interakcji z AI.

Dostawcy systemów AI, w tym tych ogólnego zastosowania, generujących treści w postaci syntetycznych dźwięków, obrazów, wideo lub tekstu, także mają obowiązek zapewnić, aby wyniki systemu AI zostały oznakowane w formacie nadającym się do odczytu maszynowego i były wykrywalne jako sztucznie wygenerowane lub zmanipulowane.

Do powyższych zasad wyjątek stanowią systemy, których wykorzystywanie jest dozwolone na mocy prawa do celów wykrywania przestępstw, przeciwdziałania im, prowadzenia postępowań przygotowawczych w ich sprawie lub ścigania ich sprawców, z zastrzeżeniem odpowiednich zabezpieczeń w zakresie praw i wolności osób trzecich. Dotyczy to także systemów, które wspomagają standardową edycję czy też nie zmieniają w sposób istotny danych wejściowych lub ich semantyki. Z wyjątkiem systemów AI wykorzystywanych w celach związanych z wykrywaniem i zapobieganiem przestępstwom, obowiązek ujawnienia, że treści zostały sztucznie wygenerowane lub zmanipulowane dotyczy również podmiotów stosujących system AI, który:

- generuje obrazy, treści audio lub wideo stanowiące deepfake – czyli takie, które przypominają istniejące osoby, przedmioty, miejsca, podmioty lub zdarzenia, które odbiorca mógłby niesłusznie uznać za autentyczne lub prawdziwe,
- generuje tekst publikowany w celu informowania społeczeństwa o sprawach leżących w interesie publicznym lub manipuluje takim tekstem – chyba że treści wygenerowane przez AI zostały poddane weryfikacji przez człowieka lub kontroli redakcyjnej i gdy za publikację treści odpowiedzialność redakcyjną ponosi osoba fizyczna lub prawna.

Karą za nieprzestrzeganie stosowania zakazanych praktyk w zakresie AI jest administracyjna kara pieniężna w wysokości do **35 mln EUR** lub w przypadku przedsiębiorstwa – w wysokości **do 7% jego całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego, w zależności od tego, która z tych kwot jest wyższa.

Następne kroki

Wersja Ogólna

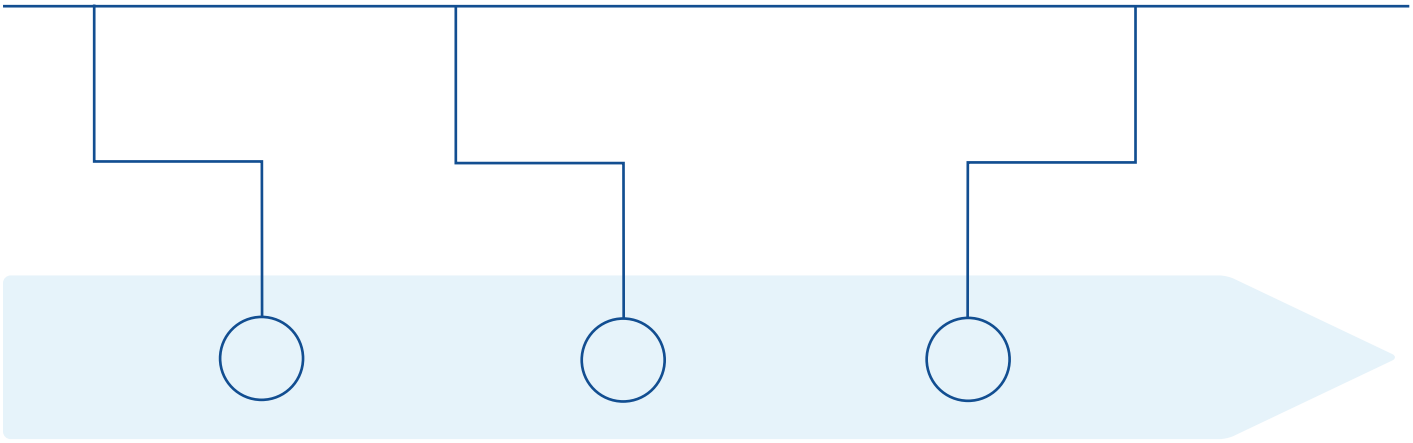
Opublikowanie AI Act

Wejście w życie

- 21 dni od ogłoszenia

Stosowanie przepisów AI Act

- Rozdziały I (Przepisy ogólne) i II (Zakazane praktyki) – od 2 lutego 2025 r.
- Rozdział III sekcja 4 (Systemy wysokiego ryzyka – Organy notyfikujące i jednostki notyfikowane), rozdział V (Modele ogólnego przeznaczenia), rozdział VII (Zarządzanie), rozdział XII (Kary) bez art. 101, art.78 – od 2 sierpnia 2025 r.
- art. 6(1) (Systemy wysokiego ryzyka) i odpowiadające mu obowiązki – od 2 sierpnia 2027 r.
- pozostałe rozdziały i artykuły – od 2 sierpnia 2026 r.



WERSJA 2 – WYBRANE SZCZEGÓŁY STOSOWANIA PRZEPISÓW

Rozdział II (Zakazane praktyki) – **od 2 lutego 2025 r.**

Rozdział V (Modele ogólnego przeznaczenia), rozdział XII (Kary) bez art. 101 – **od 2 sierpnia 2025 r.**

Art. 6(2) i Aneks III (Systemy wysokiego ryzyka), rozdział IV (obowiązki w zakresie przejrzystości) – **od 2 sierpnia 2026 r.**

art. 6(1) (Systemy wysokiego ryzyka) i odpowiadające mu obowiązki – **od 2 sierpnia 2027 r.**