Związek Banków Polskich

Akt w sprawie sztucznej inteligencji („AI Act")

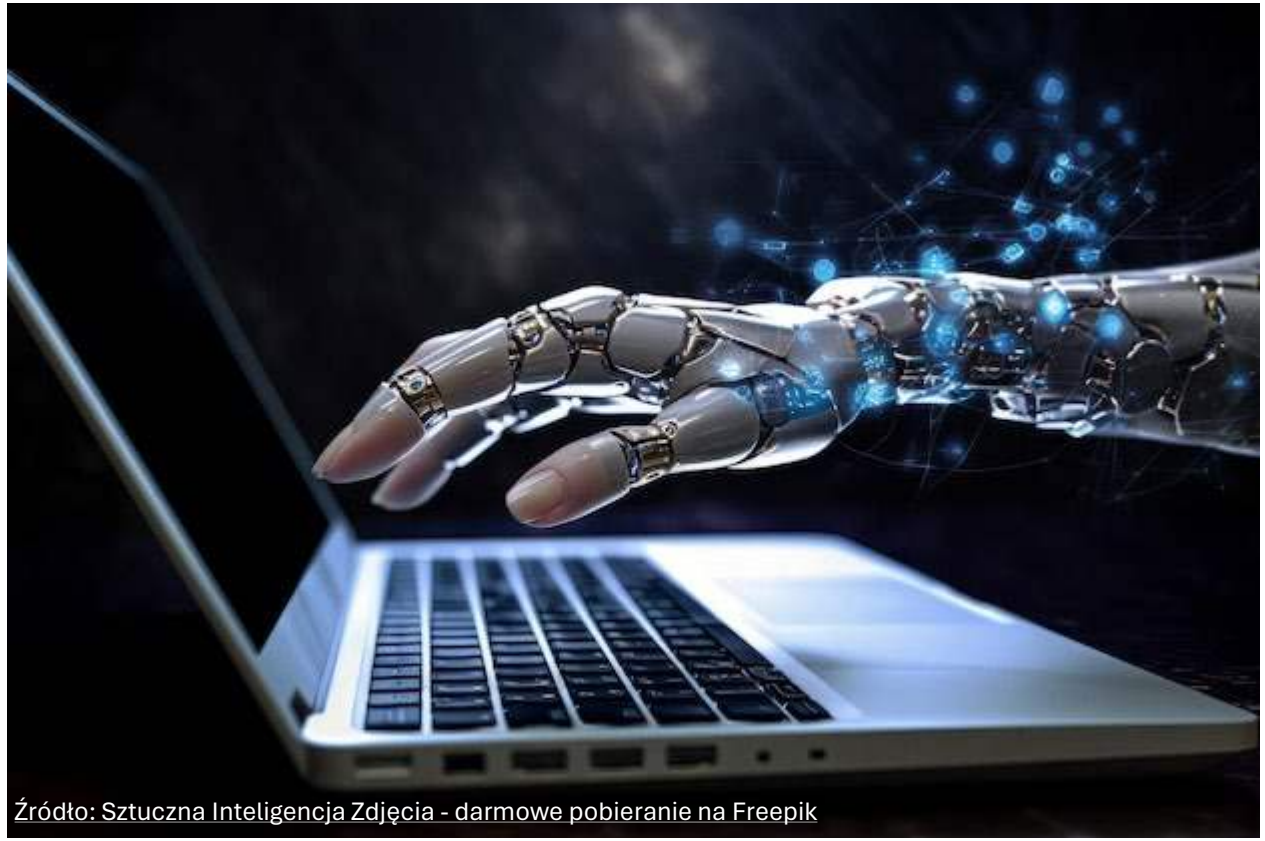
Forum Bezpieczeństwa Banków 2024

8 maja 2024

Katarzyna Urbańska
Dyrektor Zespołu Prawno-Legislacyjnego
Związek Banków Polskich

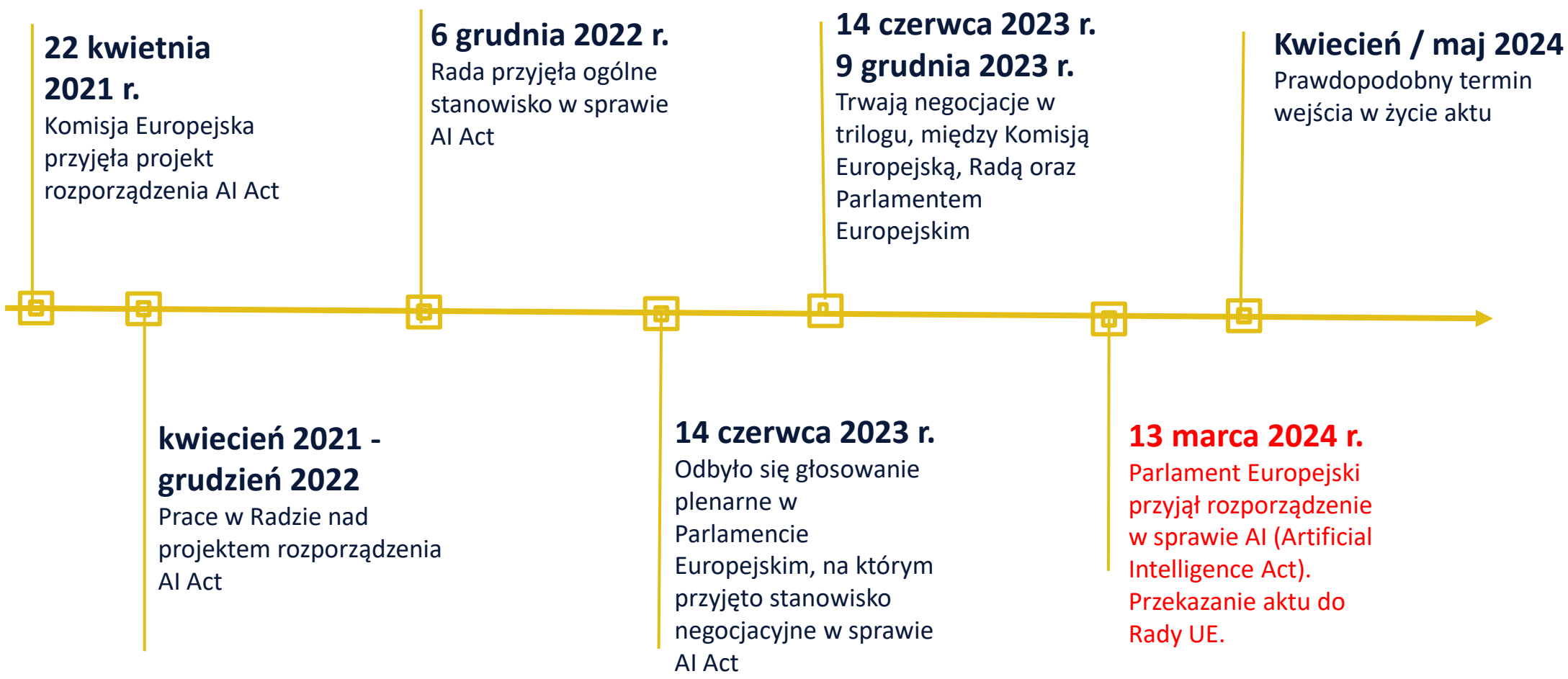
Akt w sprawie sztucznej inteligencji (AI Act)

- Pierwsze na świecie prawo dotyczące sztucznej inteligencji.
- Dotyczy podmiotów publicznych, jak i prywatnych, z UE i spoza niej, jeśli system AI wykorzystywany jest na rynku UE, bądź wpływa na obywateli UE.



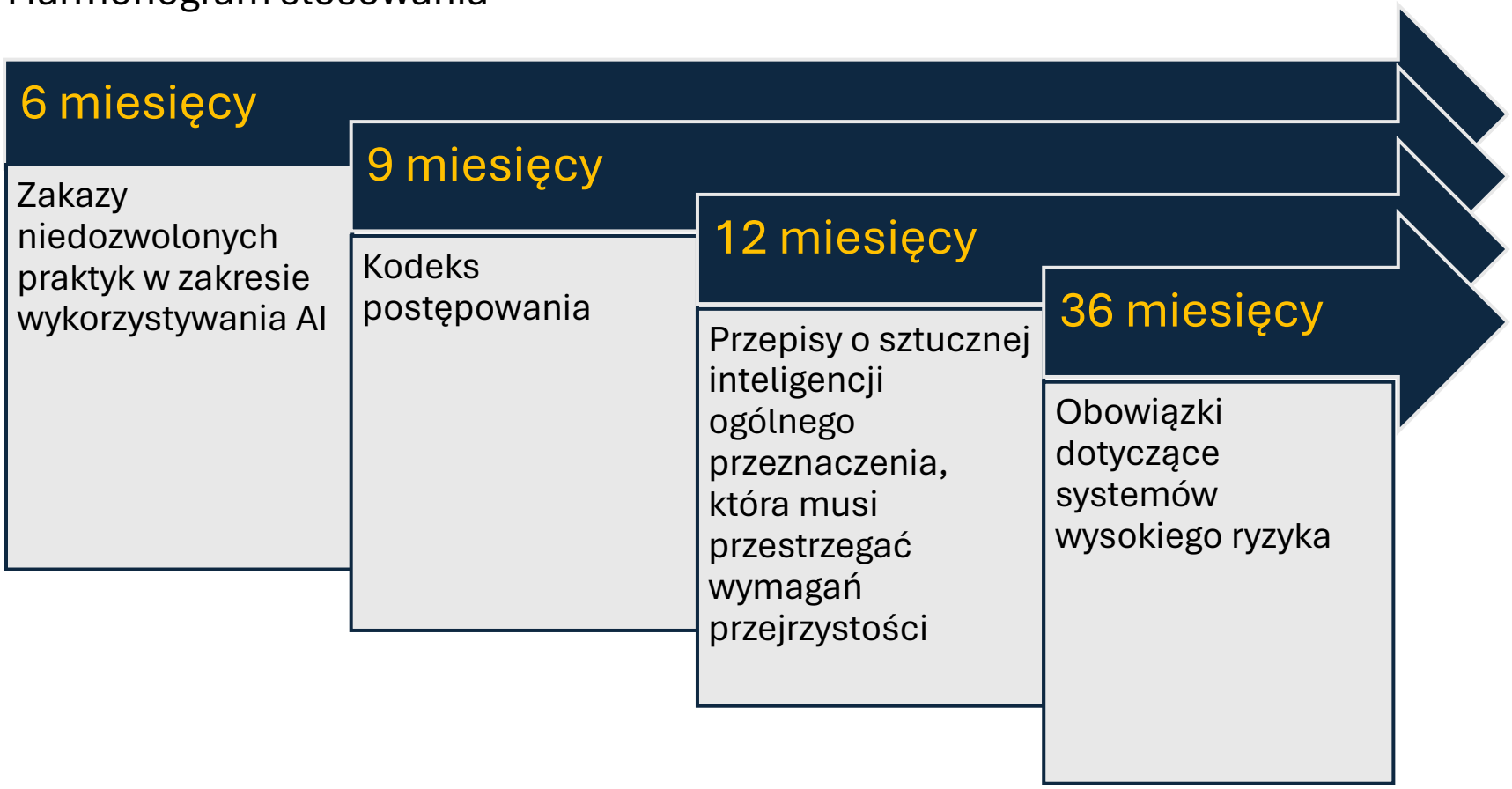
Źródło: Sztuczna Inteligencja Zdjęcia - darmowe pobieranie na Freepik

Jak wyglądały prace legislacyjne nad projektem AI ACT



AI Act ma w pełni obowiązywać 24 miesiące od dnia jego wejścia w życie

Harmonogram stosowania



*18 miesięcy od dnia wejścia w życie KE ma wydać wytyczne do AI Act

Definicja systemu AI

Źródło: Sztuczna Inteligencja Zdjęcia - darmowe pobieranie na Freepik

„System AI to system zaprojektowany do działania w sposób częściowo autonomiczny, który po wdrożeniu może wykazywać zdolność adaptacji, i który dla celów jawnych lub ukrytych, wnioskuje w oparciu o dostarczone dane w jaki sposób generować wyniki, takie jak przewidywania, treści zalecenia lub decyzje, które mogą mieć wpływ na środowisko fizyczne lub wirtualne”.

AI Act wykorzystuje podejście oparte na ryzyku

Różne przepisy dla różnych poziomów ryzyka

Rozwiązania AI o niedopuszczalnym ryzyku

Zabronione

Systemy AI wysokiego ryzyka

Będą oceniane przed wprowadzenie na rynek, a także przez cały cykl życia

Systemy sztucznej inteligencji o ograniczonym ryzyku

Dozwolone, z zastrzeżeniem wymogów przejrzystości

Sztuczna inteligencja niskiego ryzyka

Dozwolona

Rozwiązania AI o niedopuszczalnym ryzyku

Systemy sztucznej inteligencji stwarzające niedopuszczalne ryzyko, czyli uważane za zagrożenie dla ludzi, to m.in.:

- Kontrola i szkodliwe techniki podprogowe
- Wykorzystywanie słabości określonej grupy osób ze względu na wiek, niepełnosprawności lub zaburzenia psychiczne
- Scoring społeczny: klasyfikacja ludzi na podstawie ich zachowań, statusu społeczno-ekonomicznego lub cech osobistych.
- Identyfikacja biometryczna w czasie rzeczywistym i zdalnie, z wyjątkami...

Rozwiązania AI o wysokim ryzyku

Systemy sztucznej inteligencji negatywnie wpływające na bezpieczeństwo lub prawa podstawowe, lub są szkodliwe dla zdrowia będą uznane za systemy wysokiego ryzyka.

1. Systemy AI stosowane w produktach i objęte unijnymi przepisami o bezpieczeństwie produktów, np. zabawki, samochody

2. Systemy AI należące do ośmiu konkretnych obszarów, które będą musiały zostać zarejestrowane w unijnej bazie danych:
   - ❑ **Identyfikacja biometryczna**
   - ❑ Infrastruktura krytyczna
   - ❑ Edukacja i szkolenie zawodowe
   - ❑ Zatrudnienie, zarządzanie pracownikami i dostęp do narzędzi samozatrudnienia
   - ❑ Wymiar sprawiedliwości i procesy demokratyczne
   - ❑ Dostęp do usług publicznych i prywatnych
   - ❑ Egzekwowanie prawa
   - ❑ Migracja, azyl i kontrola granic

!

- *Nie obejmuje to systemów AI przeznaczonych do stosowania przy weryfikacji biometrycznej, której jedynym celem jest potwierdzenie, że określona osoba fizyczna jest osobą, za którą się podaje;*
- *Nie obejmuje to systemów AI wykorzystywanych w celu wykrywania oszustw finansowych;*

Pozostałe Rozwiązania AI

Rozwiązania AI o ograniczonym ryzyku

Są dozwolone z zastrzeżeniem wymogów przejrzystości!

- ❑ Wchodzące w bezpośrednią interakcję z osobami fizycznymi np. chatboty
- ❑ Wszelkie systemy generujące obrazy, treści dźwiękowe lub wideo, etc.
- ❑ Rozpoznawanie emocji, dokonujące kategoryzacji biometrycznej.

„(...) Przejrzystość oznacza, że systemy AI opracowuje się i wykorzystuje w sposób umożliwiający odpowiednią identyfikowalność i wytłumaczalność, jednocześnie informując ludzi o tym, że komunikują się z systemem AI lub podejmują z nim interakcję, a także należycie informując podmioty stosujące AI o możliwościach i ograniczeniach tego systemu AI, a osoby, na które AI ma wpływ, o przysługujących ich prawach”.

Rozwiązania AI o niskim ryzyku

Pozostałe systemy, które nie należą do żadnej z powyższych kategorii

Źródło: Sztuczna Inteligencja Zdjęcia - darmowe pobieranie na Freepik

Minimalne wymogi prawne w stosunku do AI wysokiego ryzyka

Wymogi wskazane w AI Act:

- **System zarządzania ryzykiem** – w odniesieniu do każdego AI wysokiego ryzyka powinien zostać opracowany, wdrożony **i utrzymany przez cały cykl życia systemu AI**, system zarządzania ryzykiem;
- **Wymogi zarządzania danymi** – AI wysokiego ryzyka, które obejmują techniki obejmujące trenowanie modeli z wykorzystaniem danych, muszą spełniać wymogi dotyczące ich wykorzystywania;
- **Dokumentacja techniczna** – jeszcze przed oddaniem AI wysokiego ryzyka do użytku, sporządza się odpowiednią dokumentację techniczną;
- **Rejestrowanie zdarzeń** – AI wysokiego ryzyka muszą być zaprojektowane tak, aby automatycznie rejestrowały pewne zdarzenia i prowadziły ich rejestr (m.in. data i godzina logowania, dane dot. identyfikacji osób fizycznych);

Źródło: Sztuczna Inteligencja Zdjęcia - darmowe pobieranie na Freepik

Minimalne wymogi prawne w stosunku do AI wysokiego ryzyka

- **Przejrzystość i dostępność danych dla użytkowników** – AI wysokiego ryzyka powinny cechować się odpowiednim stopniem przejrzystości, w tym umożliwiać użytkownikom interpretację wyników działania;
- **Nadzór człowieka** – AI wysokiego ryzyka powinny być tak zaprojektowane, aby na każdym etapie ich funkcjonowania był możliwy nadzór ze strony osoby fizycznej.
- **Dokładność, solidność i cyberbezpieczeństwo** – AI wysokiego ryzyka muszą być zaprojektowane w taki sposób, by m.in. były wolne od błędów i niespójności oraz odpowiednio zabezpieczone przed nieuprawnionym wpływem na ich funkcjonowanie przez nieupoważnione osoby.

Źródło: Sztuczna Inteligencja Zdjęcia - darmowe pobieranie na Freepik

Kary w przypadku naruszeń

Do 35 mln EUR

Nieprzestrzeganie zakazów dotyczących praktyk w zakresie sztucznej inteligencji określonych w art. 5 podlega administracyjnej karze pieniężnej w wysokości do 35 mln EUR lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do 7% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Do 10 mln EUR

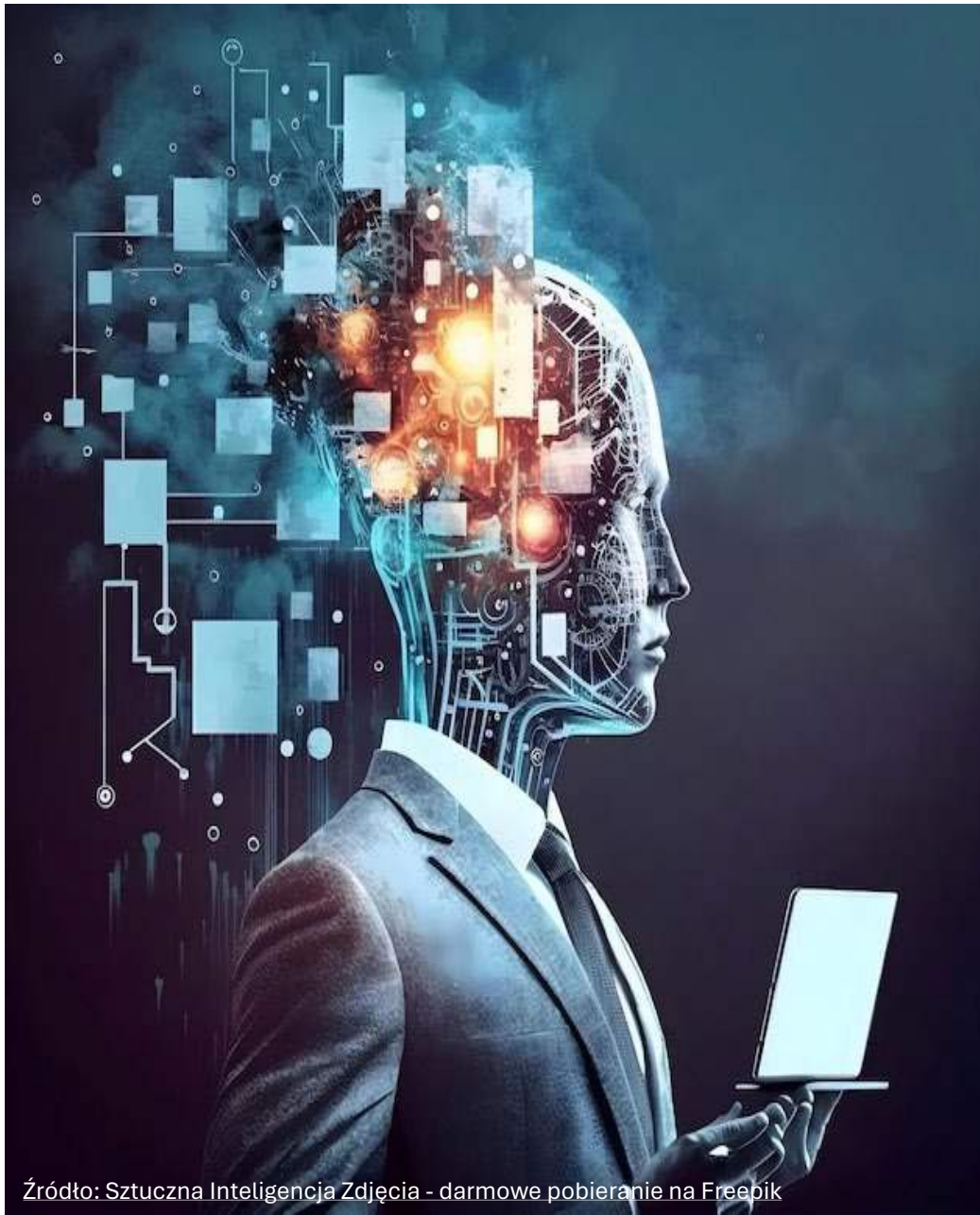
Niezgodność systemu AI z jakimikolwiek wymogami dotyczącymi operatorów lub jednostek notyfikowanych, innymi niż określone w art. 5, podlega administracyjnej karze pieniężnej w wysokości do 10 mln EUR lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do 3% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Do 7.5 mln EUR

Przekazywanie nieprawdziwych, niekompletnych lub wprowadzających w błąd informacji jednostkom notyfikowanym lub organom nadzorczym – do 7.5 mln EUR lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do 1% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Co będzie największym wyzwaniem dla banków?

- Wdrożenie AI Act?
- Interakcja z innymi regulacjami, takimi jak RODO, DORA, NIS2, MICA, AML, CCD2?
- Interdyscyplinarność?
- Bycie w zgodności z obowiązującym prawem?
- Niepewność związana ze zmianami otoczenia prawnego?
- Przeregulowanie nowoczesnych technologii w UE w odróżnieniu do Azji?
- Brak kontroli nad algorytmami?
- Odpowiedzialność banków za rezultaty AI?
- Sankcje, kary, roszczenia odszkodowawcze za zastosowanie AI?



Źródło: Sztuczna Inteligencja Zdjęcia - darmowe pobieranie na Freepik

ZWIĄZEK BANKÓW POLSKICH

Dziękuję za uwagę
i zapraszam na panel!

Związek Banków Polskich

Ul. Kruczkowskiego 8
00-380 Warszawa

Katarzyna Urbańska
Dyrektor Zespołu Prawno-Legislacyjnego

katarzyna.urbanska@zbp.pl

www.zbp.pl