Deloitte.

Szczegółowa analiza
Unijny Akt o sztucznej inteligencji

MAKING AN IMPACT THAT MATTERS since 1845

1. Wprowadzenie

Jednym z kluczowych priorytetów politycznych Komisji Europejskiej na lata 2019–2024 było stworzenie „Europy na miarę ery cyfrowej". W ramach tego ambitnego programu pod dyskusję poddano ponad 10 istotnych regulacji cyfrowych dotyczących takich obszarów, jak gospodarka oparta na danych, cyberbezpieczeństwo oraz uregulowanie funkcjonowania platform cyfrowych. Akt w sprawie sztucznej inteligencji (Akt AI) jest kluczowym elementem złożonych unijnych regulacji cyfrowych, które mają na celu ustanowienie kompleksowych ram, uwzględniających złożoność i potencjalne zagrożenia związane ze stosowaniem systemów AI. Poniższe opracowanie koncentruje się na Akcie AI, jednak za każdym razem należy je rozpatrywać w szerszym kontekście, biorąc pod uwagę cały unijny krajobraz regulacyjny dot. cyfryzacji.

Celem rozporządzenia jest wprowadzenie jednolitych założeń ramowych z myślą o uregulowaniu procesu wdrażania i wykorzystywania sztucznej inteligencji w Unii Europejskiej oraz zestandaryzowanie procesu wprowadzania jednozadaniowych systemów AI na rynek (single-purpose AI, SPAI) oraz ich aktywacji, a tym samym zapewnienie spójnego podejścia we wszystkich państwach członkowskich UE. Akt w sprawie sztucznej inteligencji, zawierający przepisy dotyczące bezpieczeństwa produktów, uwzględnia podejście oparte na ryzyku, które zakłada przypisanie poszczególnych systemów AI do odpowiednich kategorii na podstawie ich przypadku wykorzystania. Jednocześnie wprowadza wymogi zgodności w zależności od poziomu ryzyka, jakie dany system stwarza dla użytkowników.
W konsekwencji oznacza to wprowadzenie zakazu określonych zastosowań AI uznanych za nieetyczne lub szkodliwe. Rozporządzenie określa również szczegółowe wymogi wobec zastosowań wysokiego ryzyka, co ma pomóc w skutecznym zarządzaniu potencjalnymi zagrożeniami. Zawiera też przejrzyste wytyczne dotyczące stosowania technologii AI, które stwarzają ograniczone ryzyko. Zgodnie z podejściem opartym na ryzyku, głównym przedmiotem regulacji są aspekty etyczne stosowania sztucznej inteligencji. Założeniem ustawy jest możliwość zastosowania jej postanowień do nieznanych jeszcze wersji technologii AI.

Powszechne stosowanie systemów sztucznej inteligencji ogólnego przeznaczenia skłoniło ustawodawcę do dokonania rozróżnienia między jednozadaniowymi modelami AI a systemami ogólnego przeznaczenia. Akt w sprawie sztucznej inteligencji reguluje proces wprowadzania modeli AI ogólnego przeznaczenia do obrotu, niezależnie od kategorii przypadku wykorzystania określonej na podstawie analizy ryzyka. Tym samym, ramy regulacyjne ustanawiają kompleksowe zasady nadzoru nad rynkiem, zarządzania nim i egzekwowania odpowiednich postanowień aktu w celu zapewnienia integralności i zaufania publicznego wobec innowacji w zakresie AI.

Ze względu na swój abstrakcyjny charakter, rozporządzenie dotyczy obszarów, które nie zostały jeszcze w pełni zdefiniowane. Oczekuje się, że zostaną one rozwinięte w drodze aktów delegowanych i wykonawczych, wytycznych instytucji UE, a także zharmonizowanych norm opracowanych przez europejskie organizacje normalizacyjne (ESO). W związku z tym, firmy mogą spodziewać się bardziej szczegółowych wytycznych w niedalekiej przyszłości.

Przepisy weszły w życie 1 sierpnia 2024 r. Jest to początek etapowego procesu wdrażania przepisów i obowiązków wynikających z Aktu AI. Firmom pozostanie więc niewiele czasu na przygotowanie się do spełnienia obowiązku zapewnienia zgodności.

2. Zakres stosowania Aktu w sprawie sztucznej inteligencji

W tym rozdziale przyjrzymy się zakresowi prawnemu Aktu w sprawie sztucznej inteligencji oraz technologii zdefiniowanej w rozporządzeniu jako sztuczna inteligencja. Z perspektywy podmiotów z sektora publicznego i przedsiębiorstw w całej Unii Europejskiej zrozumienie tych aspektów ma kluczowe znaczenie dla zapewnienia zgodności z przepisami i wspierania innowacji w zakresie AI, przy jednoczesnym poszanowaniu norm etycznych i wartości społecznych.

2.1 Definicja sztucznej inteligencji

Celem Unii Europejskiej było sformułowanie jasnej definicji systemów sztucznej inteligencji, ściśle dostosowanej do terminologii wypracowanej przez inne organy międzynarodowe, takie jak Organizacja Współpracy Gospodarczej i Rozwoju (OECD). Przyjęcie tego rodzaju podejścia miało zagwarantować pewność prawa, ułatwić osiągnięcie spójności i akceptacji na poziomie międzynarodowym.

Zgodnie z definicją zawartą w Akcie AI, system sztucznej inteligencji to rodzaj technologii zaprojektowanej do wnioskowania, sugerowania treści lub decyzji, które mogą wpływać zarówno na środowisko fizyczne, jak i wirtualne. W tym celu wykorzystuje się różnego rodzaju technologie, w tym uczenie maszynowe (ML) - dziedzinę AI opartą na założeniu, że systemy mogą „uczyć się" poprzez analizę zbiorów danych i identyfikowanie logicznych wzorców w oparciu o określone reguły i zasady. Z uwagi na poziom autonomii, modele ML mogą funkcjonować jako samodzielne narzędzia lub jako część platformy - zintegrowany lub niezależnie funkcjonujący element innego produktu. Ich zdolność adaptacyjna odnosi się do umiejętności samodzielnego dostosowywania się do zmian, w tym wypadku zamian oznacza zasilenie nowymi danymi.

Ponadto, w części opisowej Aktu (tzw. motywy), która zawiera szczegóły aktu wykonawczego, podkreślono, że definicja sztucznej inteligencji nie obejmuje podstawowego tradycyjnego oprogramowania ani programowania opartego na regułach stworzonego przez człowieka. Mimo to jej zakres pozostaje szeroki i uwzględnia większość systemów dostępnych na rynku.

Komisji powierzono również zadanie opracowania wytycznych dotyczących stosowania definicji systemu AI zawartej w rozporządzeniu.

Definicja sztucznej inteligencji w Akcie w sprawie sztucznej inteligencji

„System AI oznacza 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."

2.2 Akt w sprawie sztucznej inteligencji rozporządzeniem dot. eksterytorialnego bezpieczeństwa produktów

Akt w sprawie sztucznej inteligencji wpływa na wszystkich operatorów systemów AI (zob. rozdział 10), w tym na pomioty prywatne i publiczne, oferujące produkty lub usługi AI na rynkach Unii Europejskiej, bez względu na ich wielkość czy sektor, w którym funkcjonują. Głównym celem regulacji jest upowszechnienie godnej zaufania sztucznej inteligencji przy jednoczesnym zapewnieniu obywatelom Unii Europejskiej wysokiego poziomu ochrony zdrowia, bezpieczeństwa i praw podstawowych.

Rozporządzenie swoim zakresem obejmuje również przedsiębiorstwa spoza UE, które wprowadzają na rynki europejskie produkty AI. Co prawda nowe przepisy nie przewidują wyłączeń dla mniejszych przedsiębiorstw, jednak w jego treści uwzględniono interesy małych i średnich przedsiębiorstw (MŚP). Na rys. 1 przedstawiono podmioty objęte Aktem AI oraz przypadki wykorzystania spoza zakresu regulacji.

Rys. 1 – Zakres stosowania

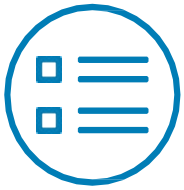
1. Zakres stosowania

Postanowienia Aktu w sprawie sztucznej inteligencji mają zastosowanie do

- Dostawców (zob. rozdział 4.1), którzy wprowadzają systemy sztucznej inteligencji do obrotu na rynku Unii Europejskiej, niezależnie od tego, czy dostawcy ci mają siedzibę lub znajdują się w Unii.
- 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.
- Podmiotów stosujących (zob. rozdział 4.1) systemy AI, które to podmioty mają siedzibę lub znajdują się w Unii;
- Importerów i dystrybutorów systemów AI w Unii Europejskiej.
- Producentów wprowadzających produkty z wbudowanymi systemami AI do obrotu na terenie Unii Europejskiej pod swoim znakiem towarowym.

2. Zasięg eksterytorialny

- Akt AI dotyczy wszystkich podmiotów lub organizacji, niezależnie od lokalizacji ich siedziby, które oferują systemy AI mające wpływ na użytkowników w Unii Europejskiej.
- Niniejszego rozporządzenia nie stosuje się do organów publicznych i organizacji międzynarodowych znajdujących się w państwie trzecim.



3. Wyłączenia

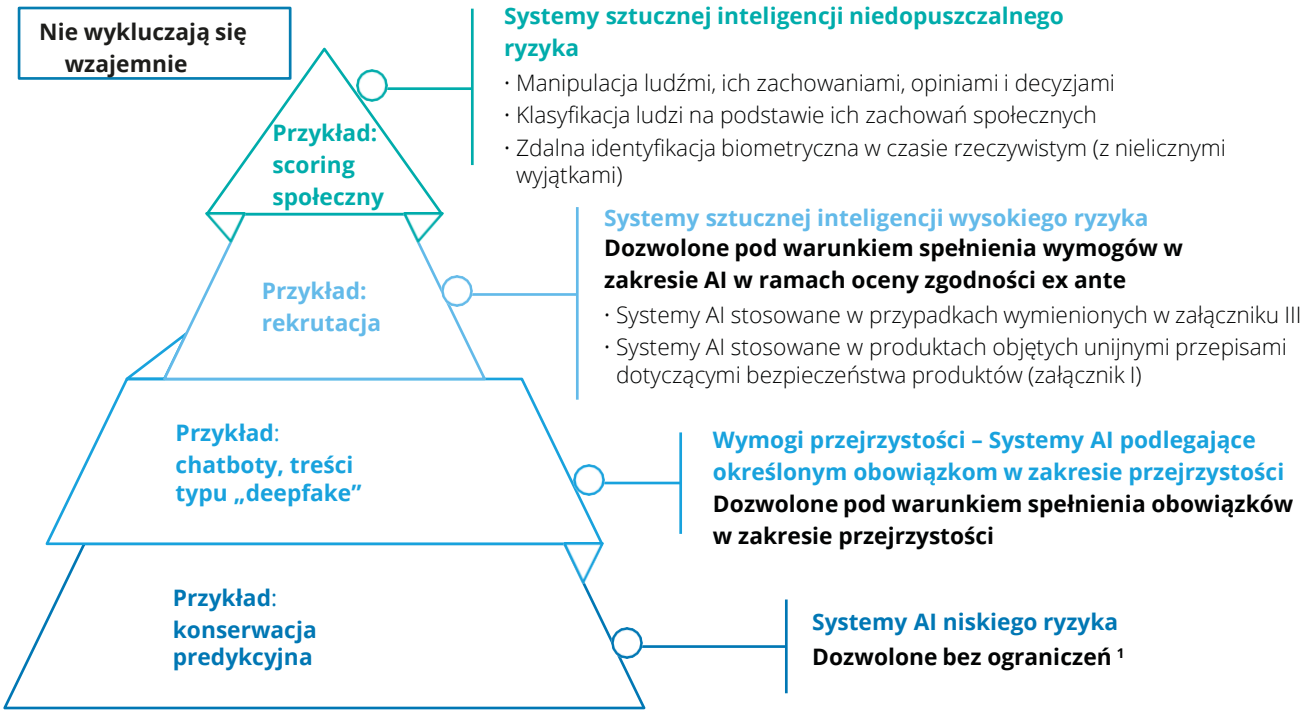
Rozporządzenie nie obejmuje niektórych przypadków wykorzystania i podmiotów:

- działalności badawczej lub rozwojowej dotyczącej systemów AI przed wprowadzeniem ich do obrotu lub oddaniem ich do użytku.
- systemów AI udostępnianych na podstawie bezpłatnych licencji otwartego oprogramowania, chyba że systemy te są wprowadzane do obrotu lub oddawane do użytku jako systemy AI wysokiego ryzyka lub stwarzające nieakceptowalne ryzyko lub jako modele AI ogólnego przeznaczenia o dużym oddziaływaniu.
- systemów AI wykorzystywanych do celów wojskowych lub obronnych.
- systemów AI opracowanych wyłącznie do celów badań naukowych i rozwojowych.
- systemów AI, które zostały wprowadzone do obrotu przed datą obowiązywania Aktu w sprawie sztucznej inteligencji; przy czym postanowienia Aktu AI będą miały zastosowanie, jeśli dany system AI zostanie istotnie zmieniony.
- systemów AI wykorzystywanych w ramach osobistej działalności pozazawodowej.

3. Jednozadaniowe modele AI - zróżnicowanie pod względem ryzyka

Akt w sprawie sztucznej inteligencji nie koncentruje się na technologii AI samej w sobie, lecz na sposobie, w jaki sztuczna inteligencja jest wykorzystywana. W tym celu przeprowadza się klasyfikację ryzyka stosowanych systemów AI, bazując na odpowiednich ramach regulacyjnych. Oznacza to, że im wyższy poziom ryzyka, tym większy zakres obowiązków do spełnienia. W regulacji określono cztery konkretne kategorie ryzyka, wraz z zestawem wymogów, tj. kategorię niedopuszczalnego ryzyka, kategorię wysokiego ryzyka, wymagania przejrzystości i kategorię niskiego ryzyka. Oczekuje się, że przedsiębiorstwa poddadzą się procesowi oceny swoich systemów AI w celu określenia kategorii ryzyka, do której dane systemy się zaliczają (patrz rys. 2).

Rys. 2 Klasyfikacja ryzyka wg. Aktu AI wraz z czterema poziomami obowiązków



[1] Stosowanie systmów AI niskiego ryzyka w dalszym ciągu może wiązać się z ryzykiem regulacyjnym, biznesowym i zagrożeniem dla bezpieczeństwa.

3.1 Zabronione zastosowania AI, które poważnie naruszają prawa osób fizycznych

Pomimo korzyści płynących z rozmaitych zastosowań sztucznej inteligencji, decydenci mają świadomość możliwości niewłaściwego jej wykorzystania, które może zagrażać fundamentalnym wartościom, takim jak poszanowanie ludzkiej godności, wolności, równości, demokracji, prywatności danych i praworządności. W tym celu podjęli kroki, aby ochronić podstawowe wartości, których rezultatem jest Akt w sprawie sztucznej inteligencji, zakazujący określonych zastosowań AI. Zakaz stosowania tego rodzaju systemów wejdzie w życie sześć miesięcy po wejściu Aktu w sprawie sztucznej inteligencji w życie tj. 1 lutego 2025 r.

Tabela 1 – Zabronione zastosowania AI

Kategorie	Przypadki wykorzystania
 **Techniki manipulacyjne oparte na AI**	nakłanianie osób do niepożądanych zachowań, skłanianie ich do podejmowania decyzji w sposób, który podważa i ogranicza ich autonomię, decyzyjność i swobodę wyboru lub z uzasadnionym prawdopodobieństwem wyrządza im szkodę; z wyłączeniem: powszechnych i zgodnych z prawem praktyk handlowych, np. w dziedzienie reklamy.
 **Kategoryzacja biometryczna**	wykorzystanie danych biometrycznych osób fizycznych, takich jak twarz lub odciski palców, w celu wydedukowania lub wywnioskowania informacji na temat opinii politycznych, przynależności do związków zawodowych, przekonań religijnych lub filozoficznych, rasy, życia seksualnego lub orientacji seksualnej danej osoby; Z wyłączeniem: etykietowania, filtrowania lub kategoryzacji zbiorów danych biometrycznych. ocena lub klasyfikacja osób fizycznych lub grup na podstawie wielu punktów danych dotyczących ich zachowań społecznych, co może doprowadzić do niekorzystnego traktowania;
 **Scoring społeczny**	z wyłączeniem: zgodnych z prawem praktyk w zakresie oceny osób fizycznych dokonanej w określonym celu zgodnie z prawem krajowym i unijnym. w przestrzeni publicznej w celu ścigania przestępstw
 **Zdalna identyfikacja biometryczna w czasie rzeczywistym**	oprócz wyjątków wymienionych w załączniku II
 **Ocena ryzyka osób fizycznych**	ocena cech osobowościowych i cech charakterystycznych w celu przewidywania ryzyka popełnienia przestępstwa; chyba że w oparciu o obiektywne, możliwe do zweryfikowania fakty mające związek z przestępstwem.
 **Bazy danych służące do rozpoznawania twarzy poprzez nieukierunkowane pozyskiwanie wizerunków twarzy (ang. untargeted scraping)**	tworzenie lub rozszerzanie baz danych rozpoznawania twarzy poprzez nieukierunkowane pobieranie wizerunków twarzy z internetu lub nagrań z telewizji przemysłowej.
 **Rozpoznawanie emocji w miejscu pracy i placówkach edukacyjnych**	rozpoznawanie emocji lub zamiarów, wyciąganie wniosków dot. osób fizycznych na podstawie ich danych biometrycznych uzyskanych w miejscu pracy lub instytucji edukacyjnej; z wyłączeniem: przyczyn medycznych, takich jak terapia, oraz względów bezpieczeństwa, takich jak ocena zmęczenia pilota.

2. Akt AI i systemy AI wysokiego ryzyka

1. System AI wysokiego ryzyka

Akt w sprawie sztucznej inteligencji koncentruje się przede wszystkim na systemach sztucznej inteligencji wysokiego ryzyka, ponieważ większość obowiązków i środków ochronnych określonych w rozporządzeniu odnosi się właśnie do zastosowań sztucznej inteligencji wysokiego ryzyka. Za systemy AI wysokiego ryzyka uznaje się systemy stanowiące zagrożenie dla bezpieczeństwa lub praw podstawowych obywateli Unii Europejskiej; zważywszy na domniemane ryzyko, jakie mogą stwarzać, konieczne jest dokonywanie ocen systemów przed wprowadzeniem ich do obrotu oraz w ciągu całego cyklu ich życia.

Rozporządzenie określa zasady klasyfikacji systemów AI jako systemów wysokiego ryzyka w podziale na dwie grupy. Pierwsza z nich obejmuje zastosowania AI wymienione w załączniku III do Aktu w sprawie sztucznej inteligencji, natomiast druga dotyczy produktów z załącznika I. W każdym przypadku podmiot, który korzysta z AI jest odpowiedzialny za samodzielne określenie, czy jego produkty lub systemy sztucznej inteligencji należą do którejś z dwóch zdefiniowanych kategorii.

Biorąc pod uwagę wysoce zindywidualizowany charakter i szybki rozwój systemów AI, szczegółowe oceny najpewniej będą przeprowadzane indywidualnie dla każdego przypadku.

Warto zauważyć, że lista zastosowań wysokiego ryzyka może podlegać rozszerzeniom i częstym aktualizacjom. Na przykład, Komisja Europejska zachowuje prawo do umieszczania nowych zastosowań AI w wykazie zastosowań sztucznej inteligencji wysokiego ryzyka za każdym razem, gdy zostaną one uznane za stwarzające zagrożenie dla zdrowia, bezpieczeństwa lub praw podstawowych obywateli Unii.

„Unijna regulacja w sprawie sztucznej inteligencji stanowi ważny krok naprzód w zakresie zarządzania sztuczną inteligencją, oferując organizacjom jasne ramy odpowiedzialnego wdrażania systemów AI. Zapewnienie zgodności z przepisami i ograniczanie ryzyka wymaga dokonywania dokładnych ocen klasyfikacji systemów AI pod kątem ryzyka, prowadzenia kompleksowego spisu zasobów AI oraz jasnego określenia ról i obowiązków każdego operatora. Postępując zgodnie z istniejącymi strukturami zarządzania ryzykiem zgodności i bezpieczeństwa, organizacje łatwiej odnajdą się w nowym krajobrazie regulacyjnym, który wprowadza solidne ramy prawne i promuje proaktywne podejście do zarządzania ryzykiem."

Czy wszystkie systemy wysokiego ryzyka są rzeczywiście obarczone wysokim ryzykiem? W celu zapewnienia, aby jedynie te systemy AI, które charakteryzują się wyraźnie podwyższonym ryzykiem były klasyfikowane jako systemy wysokiego ryzyka, wprowadzono wyjątki dla dostawców niektórych systemów AI z obszaru wysokiego ryzyka.
Systemy sztucznej inteligencji, które na pierwszy rzut oka można zaliczyć do kategorii wysokiego ryzyka, lecz w rzeczywistości nie stwarzają znaczącego ryzyka szkody dla zdrowia, bezpieczeństwa lub praw podstawowych osób fizycznych mogą, w uzasadnionych przypadkach, zostać wyłączone z kategorii sztucznej inteligencji wysokiego ryzyka. W konsekwencji są zwolnione z konieczności spełnienia wszystkich obowiązków wynikających z tego zaklasyfikowania. Zwolnienie to ma zastosowanie w przypadku, gdy:

- system AI jest przeznaczony do wykonywania wąsko określonego zadania proceduralnego.
- system AI jest przeznaczony do poprawienia wyniku zakończonej uprzednio czynności wykonywanej przez człowieka.
- system AI jest przeznaczony do wykrywania wzorców podejmowania decyzji lub odstępstw od wzorców podjętych uprzednio decyzji i nie ma na celu zastąpienia ani wywarcia wpływu na zakończoną uprzednio ocenę dokonaną przez człowieka – bez odpowiedniej weryfikacji przez człowieka.
- system AI jest przeznaczony do wykonywania zadań przygotowawczych w kontekście oceny istotnej z punktu widzenia przypadków wykorzystania systemów AI wysokiego ryzyka wymienionych rozporządzeniu.

Niemniej jednak, każdy system AI, który dokonuje profilowania osób fizycznych zawsze uznaje się za system wysokiego ryzyka. Dostawcy,

3.2.2 Zastosowania wysokiego ryzyka zgodnie z załącznikiem III

W załączniku III Aktu w sprawie sztucznej inteligencji wymieniono konkretne obszary, w przypadku których zastosowanie sztucznej inteligencji stwarza zwiększone ryzyko dla konsumentów. Wszelkie zastosowania należące do kategorii wymienionych w załączniku III, które mogą zagrażać zdrowiu, bezpieczeństwu, prawom podstawowym, środowisku, demokracji lub praworządności są automatycznie uznawane za zastosowania wysokiego ryzyka.

W związku z tym algorytmy i procesy decyzyjne w ramach systemów AI zaklasyfikowanych jako systemy wysokiego ryzyka wymagają solidnych zabezpieczeń, aby ograniczyć potencjalne szkody, chyba że należą do jednego z wyjątków (rozdział 3.2.1 dot. ocenie wyjątków). Zasady dotyczące zastosowań wysokiego ryzyka, o których mowa w załączniku III, zaczną obowiązywać po upływie 24 miesięcy od daty wejścia regulacji w życie.

Tabela 2 – Zastosowania sztucznej inteligencji wysokiego ryzyka załącznik III

Kategorie		Przypadki wykorzystania
	**Biometria**	systemy zdalnej identyfikacji biometrycznej dozwolone na podstawie odpowiednich przepisów w wyjątkowych okolicznościach określonych w załączniku II; w tym systemy AI przeznaczone do wykorzystania przy kategoryzacji biometrycznej oraz przy rozpoznawaniu emocji
	**Infrastruktura krytyczna zdefiniowana zgodnie z Dyrektywą CER**	elementy bezpieczeństwa w zarządzaniu i eksploatacji krytycznej infrastruktury cyfrowej (np. w ruchu drogowym, zaopatrzenia w wodę/gaz/ogrzewanie/energię elektryczną)
	**Kształcenie i szkolenie zawodowe**	przyjęcie do placówek wszystkich szczebli oraz ocena uzyskanego poziomu wykształcenia; wykorzystywanie systemów AI do celów oceny efektów uczenia się i kierowania procesem uczenia się osób fizycznych, oraz do monitorowania i wykrywania niedozwolonego zachowania uczniów podczas testów
	**Zatrudnienie, zarządzanie pracownikami i samozatrudnienie**	wykorzystywane do rekrutacji, na przykład analizy i filtrowania podań o pracę lub oceny kandydatów; decydowanie o awansach, rozwiązywaniu stosunku pracy lub przydzielaniu zadań; stosowane do monitorowania i oceny wydajności i zachowania pracownika
	**Podstawowe usługi publiczne i prywatne**	ocena kwalifikowalności osób fizycznych do podstawowych świadczeń i usług publicznych; ocena ryzyka i wycena w przypadku ubezpieczeń na życie i ubezpieczeń zdrowotnych; ocena zdolności kredytowej lub ustalenie scoringu kredytowego; ocena i klasyfikacja zgłoszeń alarmowych oraz ustalanie priorytetów w nagłych wypadkach
	**Ściganie przestępstw**	wykorzystywanie systemów AI w badaniach wariografem lub do oceny ryzyka stania się ofiarą przestępstwa; ocena wiarygodności dowodów i ściganie przestępstw; profilowanie w toku wykrywania, prowadzenia dochodzeń i ścigania przestępstw; ocena ryzyka popełnienia przestępstwa lub ponownego popełnienia przestępstwa przez osobę fizyczną w oparciu o profilowanie i ocenę cech behawioralnych i kryminalnych
	**Zarządzanie migracją, azylem i kontrolą graniczną**	stosowane w wariografach lub ocenie zagrożeń bezpieczeństwa; również przy rozpatrywaniu wniosków o udzielenie azylu, o wydanie wizy lub dokumentów pobytowych lub do celów wykrywania, rozpoznawania lub identyfikacji osób fizycznych
	**Sprawowanie wymiaru sprawiedliwości i procesy demokratyczne**	badanie i interpretacja stanu faktycznego i przepisów prawa; stosowanie prawa; wywieranie wpływu na wynik wyborów i zachowanie osób fizycznych podczas głosowania

3.2.3 Systemy AI jako elementy produktów związanych z bezpieczeństwem

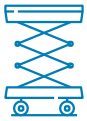
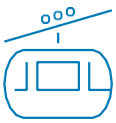
Akt w sprawie sztucznej inteligencji kładzie szczególny nacisk na produkty bezpieczeństwa z wbudowanymi systemami AI oraz związane z nimi potencjalne zagrożenia. W załączniku I do regulacji wymieniono sektory, które zostały uznane za sektory wysokiego ryzyka ze względu na ich znaczenie dla zdrowia i bezpieczeństwa osób, w przypadku gdy systemy AI satnowią element produktów związanych z bezpieczeństwem.

Zadaniem operatorów z określonych sektorów jest doprecyzowanie, czy systemy AI ujęte w Akcie są zintegrowane z produktem, stanowiąc tym samym związany z bezpieczeństwem element, oraz czy podlegają ocenie zgodności przez stronę trzecią. Zasady dotyczące zastosowań wysokiego ryzyka, o których mowa w załączniku I, zaczną obowiązywać po upływie 36 miesięcy od daty wejścia regulacji w życie. Akt w sprawie sztucznej inteligencji reguluje następujące obszary:

Tabela 3 – Zastosowania sztucznej inteligencji wysokiego ryzyka załącznik I

Kategorie		Przypadki wykorzystania
	**Lotnictwo cywilne**[2]	wszystkie porty lotnicze lub części portów lotniczych, które nie są wykorzystywane wyłącznie do celów wojskowych, a także wszyscy operatorzy, w tym przewoźnicy lotniczy, świadczący usługi w portach lotniczych lub częściach portów lotniczych, które nie są wykorzystywane wyłącznie do celów wojskowych[3]
	**Pojazdy rolnicze i leśne**[2]	ciągniki, przyczepy oraz wymienne urządzenia ciągnięte[3]
	**Pojazdy dwu- lub trzykołowe oraz czterokołowce and quadricycles**	wszystkie pojazdy dwu- lub trzykołowe oraz czterokołowce
	**Wyposażenie morskie**[2]	wyposażenie, które znajduje się lub ma być umieszczone na pokładzie statków UE
	**Ochrona indywidualna**	środki ochrony indywidualnej zaprojektowane i wyprodukowane do noszenia lub trzymania przez osobę w celu ochrony przed jednym lub większą liczbą zagrożeń dla zdrowia lub bezpieczeństwa tej osoby, jak również wymienialne elementy składowe środków oraz systemy przyłączy do środków
	**Urządzenia spalające paliwa gazowe**	urządzenia spalające paliwa gazowe używane do gotowania, chłodzenia, klimatyzacji, ogrzewania pomieszczeń, wytwarzania gorącej wody, oświetlenia lub prania, jak również osprzęt oznaczający urządzenia zabezpieczające lub urządzenia sterujące do przyłączenia do urządzenia
	**System kolei** [2]	system kolejowy, w tym pojazdy, infrastruktura, systemy energetyczne i sygnalizacyjne[3]
	**Pojazdy silnikowe i przyczepy oraz układy, komponenty i oddzielne zespoły techniczne przeznaczone do tych pojazdów** [2]	pojazdy silnikowe i ich przyczepy; w tym jazda autonomiczna[3]

[2] Sektory wymienione w Części B podlegają określonym artykułom unijnego Aktu w sprawie sztucznej inteligencji, co może wiązać się z różnicami w zastosowaniu.
[3] m.in.

Kategorie	Przypadki wykorzystania
 **Lotnictwo cywilne, europejska przestrzeń powietrzna, lądowiska** [2]	projektowania i produkcji wyrobów, części i wyposażenia do zdalnego sterowania statkami powietrznymi, przez osobę fizyczną lub prawną, jak również projektowanie, produkcja, obsługi technicznej i eksploatacji statków powietrznych[3]
 **Wyroby medyczne**	wyroby medyczne stosowane u ludzi wraz z akcesoriami, a także badania kliniczne dotyczące wyrobów medycznych i akcesoriów [3]
 **Wyroby medyczne do diagnostyki in vitro**	wyroby medyczne do diagnostyki in vitro stosowane u ludzi wraz z akcesoriami [3]
 **Maszyny**	maszyny, urządzenia wymienne i osprzęt do podnoszenia (np. roboty)[3]
 **Zabawki**	produkty zaprojektowane lub przeznaczone do użytku podczas zabawy przez dzieci poniżej 14 roku życia (np. zabawki podłączone do prądu lub urządzenia IoT)
 **Rekreacyjne jednostki pływające i skutery wodne**	rekreacyjne jednostki pływające oraz silniki napędowe instalowane na jednostkach pływających [3]
 **Dźwigi**	dźwigi stale obsługujące budynki i konstrukcje przewidziane do transportu osób lub osób i towarów
 **Urządzenia i systemy ochronne przeznaczone do użytku w atmosferze potencjalnie wybuchowej**	urządzenia i systemy ochronne przeznaczone do użytku w atmosferze potencjalnie wybuchowej, a także komponenty będące częścią urządzeń i systemów ochronnych [3]
 **Urządzenia ciśnieniowe**	projektowanie, wytwarzanie i ocena zgodności urządzeń ciśnieniowych i zespołów
 **Urządzenia radiowe**	wszelkiego rodzaju sprzęt radiowy odbierający fale radiowe (np. WiFi, Bluetooth, 5G w laptopach, telefonach, urządzeniach IoT)
 **Urządzenia kolei linowych**	nowe urządzenia kolei linowych przeznaczone do przewozu osób, do modyfikacji urządzeń kolei linowych wymagających nowego zezwolenia oraz do podsystemów i elementów bezpieczeństwa urządzeń kolei linowych

3.3 Zasady przejrzystości i inne rodzaje ryzyka

W przypadku zastosowań sztucznej inteligencji o ograniczonym ryzyku głównym wymogiem jest przestrzeganie określonych zasad dotyczących przejrzystości. Podczas gdy stosowanie niektórych systemów AI podlega jedynie określonym obowiązkom w zakresie przejrzystości, nie należy zapominać, że systemy AI należące do innych kategorii ryzyka oprócz spełnienia konkretnych wymogów regulacyjnych podlegają również przepisom dot. przejrzystości. Przykładem systemów AI o ograniczonym ryzyku są chatboty oparte na sztucznej inteligencji. W tym przypadku istotne jest zapewnienie użytkowników, że wchodzą w interakcję z maszyną oraz umożliwienie im skorzystania z obsługi konsultanta-człowieka.

Co istotne, systemy AI należące do niskiej kategorii ryzyka nie podlegają wymogom Aktu w sprawie sztucznej inteligencji. Grupa ta może obejmować znaczną część istniejących zastosowań AI w różnych sektorach, w tym filtry antyspamowe, gry wideo wykorzystujące sztuczną inteligencję i systemy zarządzania zapasami. Oznacza to, że operatorzy nie mają obowiązku przestrzegania wymogów kodeksu postępowania dot. etycznej i godnej zaufania AI w Unii. Urząd ds. AI (zob. rozdział 6) będzie wspierać i promować opracowywanie kodeksów postępowania, które będą uwzględniały istniejące rozwiązania techniczne i najlepsze praktyki branżowe.

Należy pamiętać, że systemy sztucznej inteligencji, które nie podlegają wymogom Aktu w sprawie sztucznej inteligencji w dalszym ciągu mogą stwarzać ryzyko biznesowe i ryzyko dla bezpieczeństwa i powinny spełniać obowiązki regulacyjne wynikające z innych przepisów unijnych, których nie należy lekceważyć.

4. Role i obowiązki w zależności od kategorii ryzyka

4.1 Zakres odpowiedzialności dostawców, podmiotów stosujących, dystrybutorów i importerów

Zakres odpowiedzialności poszczególnych podmiotów określony w Akcie w sprawie sztucznej inteligencji różni się w zależności od specyfiki danego operatora AI (zob. rozdział 10) - rodzaju pełnionej roli i przypadku wykorzystania. Co więcej, pomimo definicji obowiązków zawartej w regulacji dot. AI, jej ostateczny kształt będzie przedmiotem prac grup roboczych w nadchodzących latach i zostanie przyjęty przez Komisję w drodze aktów delegowanych i wykonawczych, oraz zharmonizowanych norm.

W związku z tym niezbędne jest, aby każdy operator określił odpowiednią dla siebie kategorię ryzyka. Akt AI wyodrębnia cztery główne kategorie operatorów: dostawcę, podmiot stosujący, dystrybutora i importera. Każda kategoria podlega odrębnym obowiązkom wynikającym z Aktu w sprawie sztucznej inteligencji i jest zdefiniowana w następujący sposób:

Rys. 3 - Definicje ról

Dostawca
osoba fizyczna lub prawna, organ publiczny, agencja lub inny podmiot, które rozwijają system AI lub model AI ogólnego przeznaczenia lub zlecają rozwój systemu AI lub modelu AI ogólnego przeznaczenia oraz które – odpłatnie lub nieodpłatnie – pod własną nazwą lub własnym znakiem towarowym wprowadzają do obrotu lub oddają do użytku system AI

Podmiot stosujący
osoba fizyczna lub prawna, organ publiczny, agencja lub inny podmiot, które wykorzystują system AI, nad którym sprawują kontrolę, z wyjątkiem sytuacji, gdy system AI jest wykorzystywany w ramach osobistej działalności pozazawodowej

Dystrybutor
osoba fizyczna lub prawna w łańcuchu dostaw, inna niż dostawca lub importer, która udostępnia system AI na rynku Unii

Importer
osoba fizyczna lub prawna znajdująca się lub mająca siedzibę w Unii, która wprowadza do obrotu system AI opatrzony nazwą lub znakiem towarowym osoby fizycznej lub prawnej mającej siedzibę w państwie trzecim

Szczególny przypadek dostawców:
Za dostawcę systemu AI wysokiego ryzyka i systemu AI ogólnego przeznaczenia uznaje się i obejmuje obowiązkami dostawcy każdego operatora (dystrybutora lub podmiot stosujący), jeżeli zachodzi którakolwiek z następujących okoliczności:

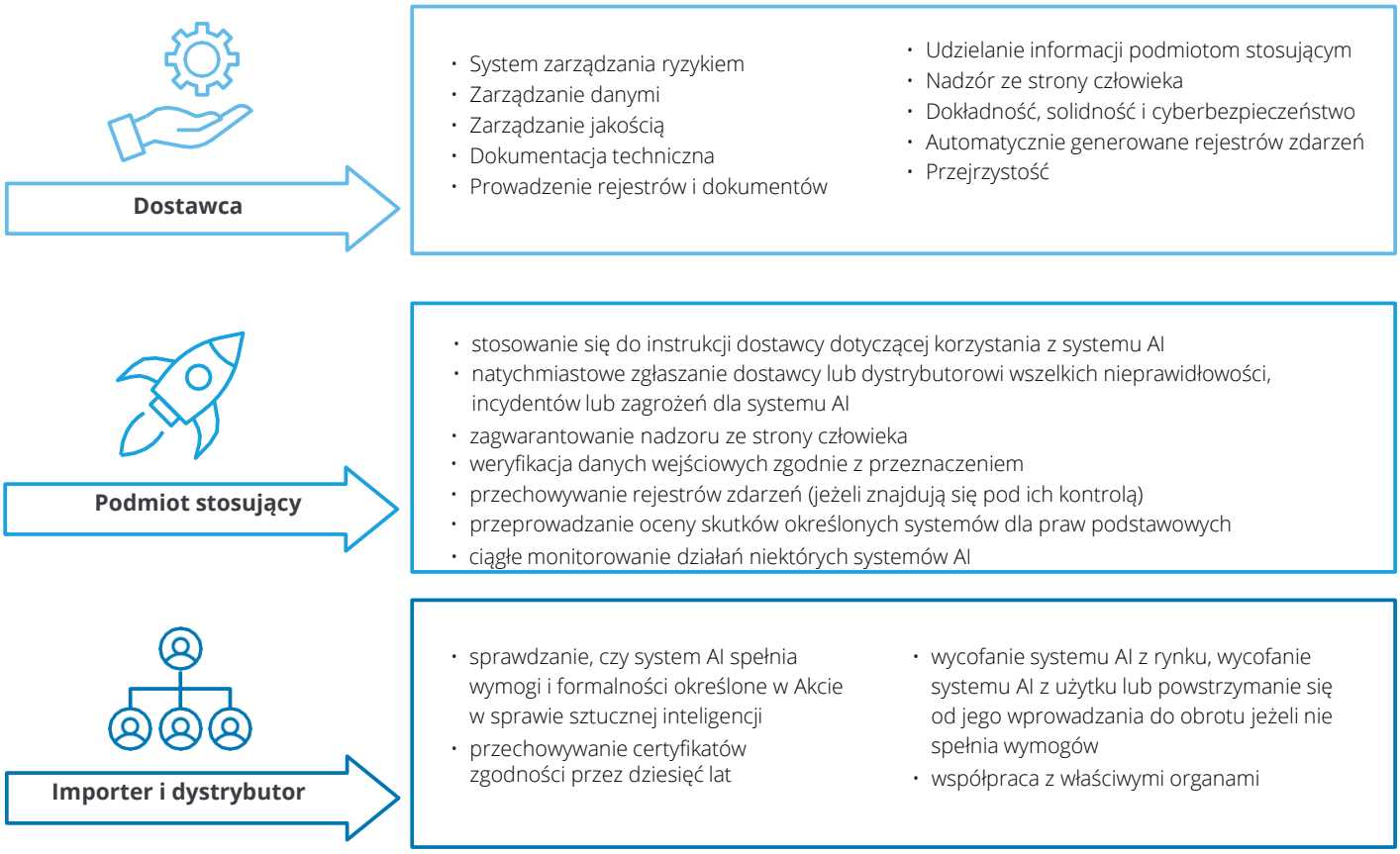
1. Jeżeli umieszczają oni swoją nazwę lub znak towarowy w systemie AI wysokiego ryzyka, który został już wprowadzony do obrotu lub oddany do użytku, bez uszczerbku dla ustaleń umownych przewidujących.
2. Jeżeli we wprowadzonym już do obrotu lub oddanym do użytku systemie AI wysokiego ryzyka dokonują oni istotnej zmiany w taki sposób, że pozostaje on systemem AI wysokiego ryzyka.
3. Jeżeli zmieniają oni przeznaczenie systemu AI, w tym systemu AI ogólnego przeznaczenia, który nie został zaklasyfikowany jako system AI wysokiego ryzyka, ale w drodze wprowadzonych modyfikacji staje się systemem AI wysokiego ryzyka.

Odrębne obowiązki w zależności od pełnionej roli

Poniższa grafika przedstawia zarys obowiązków i zadań, w podziale na poszczególnych operatorów. Finalna wersja regulacji zawiera bardziej kompleksowe opisy obowiązków, które również mogą zostać poddane dalszym doprecyzowaniom. Niemniej jednak, państwa członkowskie obowiązuje zasada wzajemnego uznawania ocen dokonywanych przez organy krajowe. Jednocześnie, każde państwo członkowskie może podjąć działania w przypadku potencjalnych naruszeń.

Dostawcy wszystkich systemów AI i podmioty je stosujące muszą zapewnić, aby ich pracownicy i osoby fizyczne, a także osoby lub grupy osób, na które AI ma wpływ, posiadali odpowiednią wiedzę na temat sztucznej inteligencji, przy uwzględnieniu ich obecnego poziomu wiedzy technicznej, wykształcenia, odbytych szkoleń i zamierzonego wykorzystania systemów AI. W Akcie w sprawie sztucznej inteligencji podkreślono znaczenie posiadania kompetencji w zakresie AI, a tym samym konieczność wyposażenia operatorów systemów AI w niezbędną wiedzę i zasoby, aby mogli podejmować świadome decyzje dotyczące systemów sztucznej inteligencji. Oznacza to nie tylko zrozumienie dokładnego zastosowania elementów technicznych na etapie rozwoju systemów AI, ale także zdobycie wiedzy na temat właściwych środków, które należy zastosować podczas używania systemów AI, oraz umiejętność prawidłowej interpretacji i właściwego wykorzystania uzyskanych wyników.

Rys. 4 – Ogólny przegląd/podsumowanie obowiązków operatorów systemów AI wysokiego ryzyka



Jednym z głównych obowiązków spoczywających na dostawcach systemów AI wysokiego ryzyka jest opracowanie systemu zarządzania ryzykiem w odniesieniu do danego systemu, który będzie obejmować wszystkie fazy cyklu życia systemu AI. Zgodnie z Aktem w sprawie sztucznej inteligencji należy zapewnić:

- **Bezpieczeństwo na etapie projektowania (ang. safety by design)** wyeliminowanie lub ograniczenie – w zakresie, w jakim jest to technicznie wykonalne – ryzyka zidentyfikowanego i ocenionego zgodnie z ust. 2 poprzez odpowiedni projekt i rozwój systemu AI wysokiego ryzyka;

- **Środki ochronne** w stosownych przypadkach – wdrożenie odpowiednich środków służących ograniczeniu i kontroli ryzyka, którego nie można wyeliminować;

- **Informacje na potrzeby bezpieczeństwa** dostarczenie informacji wymaganych zgodnie z art. 13 (Przejrzystość i udostępnianie informacji podmiotom stosującym) oraz, w stosownych przypadkach, przeszkolenie podmiotów stosujących

Kolejnym ważnym wymogiem jest ustanowienie systemu zarządzania jakością, który będzie obejmować cały cykl życia systemu AI w odniesieniu do następujących czynników:

1. Faza przed wprowadzeniem do obrotu
Obejmuje strategię na rzecz zgodności regulacyjnej, kontrolę i weryfikację projektu, badanie systemu, testowanie i walidację systemów sztucznej inteligencji oraz specyfikację techniczną.

2. Faza po wprowadzeniu do obrotu
Kontrola jakości, zgłaszanie poważnych incydentów oraz system monitorowania po wprowadzeniu do obrotu.

3. Faza ciągła
Obejmuje systemy i procedury zarządzania danymi, system zarządzania ryzykiem, komunikację z organami oraz prowadzenie dokumentacji i rejestrów, w tym rejestrów zdarzeń.
Uwzględnia również zarządzanie zasobami, w tym bezpieczeństwo dostaw oraz ramy odpowiedzialności.

4.3 Dwa rodzaje oceny zgodności na podstawie Aktu w sprawie sztucznej inteligencji

Unia Europejska ustanowiła nowe ramy prawne (NLF), zgodnie z którymi niektóre produkty zanim zostaną dopuszczone do sprzedaży, najpierw muszą zostać poddane ocenie. Wprowadzenie nowych ram prawnych ma za zadanie zapewnienie, że produkty wprowadzane do obrotu spełniają określone przepisy i normy unijne dotyczące bezpieczeństwa, jakości i wydajności. Akt w sprawie sztucznej inteligencji, będący częścią NLF, wymaga przeprowadzenia „oceny zgodności", której potwierdzeniem jest „deklaracja zgodności" - warunek wstępny, aby produkty mogły zostać wprowadzone na rynek i wykazać zgodność z odpowiednimi wymogami.

Jak czytamy w unijnym Akcie w sprawie sztucznej inteligencji ocena zgodności systemów sztucznej inteligencji wysokiego ryzyka może zostać przeprowadzona przez samych dostawców lub przy wsparciu osób trzecich. Dostawcy mogą dokonać samooceny wszystkich zastosowań systemów AI wysokiego ryzyka wymienionych w załączniku III (np. zatrudnienie, podstawowe usługi publiczne i prywatne) w oparciu o mechanizmy kontrololne oraz wystawić deklarację zgodności.

Natomiast w przypadku systemów AI wymienionych w załączniku I (np. lotnictwo, motoryzacja i wyroby medyczne) dostawcy muszą zwrócić się o wsparcie osób trzecich. Tutaj ocena zgodności musi zostać przeprowadzona przez akredytowaną „jednostkę notyfikowaną", posiadającą odpowiednie kompetencje do oceny danego rodzaju systemu AI. Jednostki notyfikowane to jednostki oceniające zgodność, wyznaczone przez organ notyfikujący. Jeżeli jednostka notyfikowana uzna system sztucznej inteligencji za zgodny, obowiązkiem dostawcy jest wystawienie deklaracji zgodności.

Jedynie dostawcy systemów biometrycznych wysokiego ryzyka mają możliwość przeprowadzenia kontroli wewnętrznej lub skorzystania z oceny strony trzeciej.

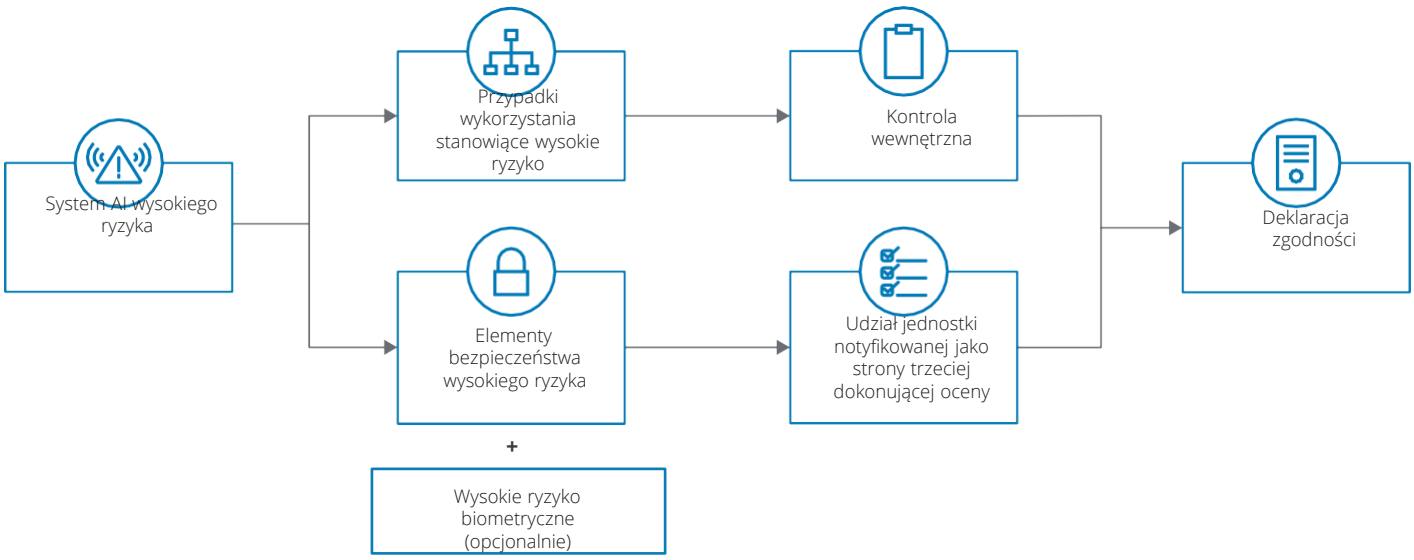
Zgodnie z założeniem dostawcy, którzy dokonują samooceny, spełniają przepisy, jeśli przestrzegają norm zharmonizowanych. Komisja wydała wnioski o normalizację, zwracając się o przedstawienie wyników sprawozdawczości i procesów dokumentowania w celu poprawy skuteczności działania zasobów systemów AI. Oczekuje się, że zharmonizowane normy zostaną opracowane jeszcze przed wprowadzeniem odpowiednich przepisów w życie. Za proces odpowiedzialny jest Europejski Komitet Normalizacyjny Elektrotechniki (CENELEC) we współpracy z Europejskim Komitetem Normalizacyjnym (CEN).

Dostawcy systemów AI wysokiego ryzyka mogą skorzystać z domniemania zgodności z obowiązkami w zakresie danych i zarządzania danymi, jeżeli dane wykorzystywane do trenowania ich systemów AI dokładnie odzwierciedlają konkretne otoczenie geograficzne, behawioralne, kontekstowe lub funkcjonalne, w których systemy te mają być wykorzystywane. Wówczas uznaje się, że dostawcy spełniają obowiązki wymienione w art. 10, co oznacza, że nie muszą przechodzić standardowych rygorystycznych procesów walidacji i testowania zbiorów danych pod kątem wyeliminowania potencjalnego ryzyka stronniczości i nierepreprezentatywnych danych treningowych.

Dodatkowo, uznaje się, że dostawcy, którzy uzyskali certyfikację lub deklarację zgodności w ramach programu certyfikacji cyberbezpieczeństwa zgodnie z unijnym aktem o cyberbezpieczeństwie spełniają wymogi w zakresie cyberbezpieczeństwa, o których mowa w art. 15.

Wszystkie zatwierdzone systemy sztucznej inteligencji wysokiego ryzyka zostaną opublikowane w ogólnounijnym rejestrze.

Rys. 5 – Ocena przez stronę trzecią vs kontrola wewnętrzna



4.4 Najważniejsze aspekty oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych

Przed wdrożeniem systemów AI wysokiego ryzyka podmioty stosujące będące podmiotami prawa publicznego lub podmiotami prywatnymi świadczącymi usługi publiczne, oraz podmioty dokonujące oceny zdolności kredytowej i oceny ryzyka w odniesieniu do polis ubezpieczeniowych na życie muszą przeprowadzić ocenę skutków dla praw podstawowych. Ocena ta obejmuje opis zamierzonego zastosowania systemu, częstotliwości użytkowania, kategorię osób fizycznych lub grup, na które wykorzystywanie systemu może mieć wpływ, ocenę potencjalnego ryzyka, opis środków nadzoru ze strony człowieka oraz szczegółowe strategie ograniczania ryzyka.

Po przeprowadzeniu oceny obowiązkiem podmiotów stosujących jest powiadomienie organu nadzoru rynku o jej wynikach. Jeżeli ocena skutków dla ochrony danych została już przeprowadzona, oceną skutków dla praw podstawowych powinna stanowić jej uzupełnienie. Urząd ds. AI opracowuje wzór kwestionariusza, aby ułatwić podmiotom stosującym spełnienia tych obowiązków. Państwa członkowskie mogą wyznaczyć lub ustanowić instytucje nadzorujące ochronę praw podstawowych - szczegółowe wyjaśnienia zamieszczono w rozdziale 6.1.

5. Odrębna kategoria ryzyka stosowana wobec systemów AI ogólnego przeznaczenia

Modele AI ogólnego przeznaczenia, trenowane na ogromnych zbiorach danych oraz zdolne do wykonywania szerokiego zakresu zadań, wzbudziły największe kontrowersje w trakcie negocjacji Aktu AI.

Zgodnie z podejściem opartym na analizie ryzyka, Akt w sprawie sztucznej inteligencji wprowadza bardziej rygorystyczne wymogi wobec systemów AI wysokiego ryzyka. Jednak to uniwersalność i wszechstronność modeli AI ogólnego przeznaczenia sprawia, że precyzyjna kategoryzacja ryzyka jest niezwykle trudna z uwagi na niejasny cel zastosowania systemów lub aplikacji niższego szczebla.

Aby rozwiązać ten problem, w ostatecznej wersji regulacji w rozdziale V pojawił się specjalny zapis dotyczący dostawców modeli AI ogólnego przeznaczenia („modele podstawowe"), a nie samych systemów. Model AI jest podstawowym elementem systemu sztucznej inteligencji, używanym do wyciągania wniosków na podstawie danych wejściowych w celu wygenerowania danych wyjściowych. Zazwyczaj ustalenie ostatecznych parametrów modelu następuje po zakończeniu fazy budowy. Dzięki temu ryzyko stwarzane przez modele AI ogólnego przeznaczenia jest łatwiejsze do oszacowania i uregulowania niż w przypadku gotowych systemów. Z uwagi na traktowanie modeli i systemów jako odrębnych elementów, sam model AI ogólnego przeznaczenia nie zostanie zaklasyfikowany jako system AI wysokiego ryzyka. Ale już system AI ogólnego przeznaczenia zbudowany na modelu AI ogólnego przeznaczenia może zostać zaliczony do jednej z ustalonych kategorii ryzyka. Dla modeli AI ogólnego przeznaczenia europejscy regulatorzy przyjęli podejście dwustopniowe, które wprowadza rozgraniczenie na obowiązki dostawców modeli AI ogólnego przeznaczenia, które stwarzają ryzyko systemowe, czyli modele wykazujące zdolność dużego oddziaływania, oraz modele, które takiego ryzyka nie generują.

Uznanie modelu AI ogólnego przeznaczenia za wykazujący zdolności dużego oddziaływania następuje na postawie oceny ryzyka systemowego. Jeżeli łączna liczba obliczeń wykorzystywanych do trenowania modelu, mierzona w operacjach zmiennoprzecinkowych, jest większa niż 1025, domniemuje się, że ma on zdolność dużego oddziaływania.
Ewentualnie, Komisja, na podstawie ostrzeżenia wydanego przez panel naukowy, może uznać model AI ogólnego przeznaczenia za model stwarzający ryzyko systemowe. W tym przypadku stosowane są kryteria oceny określone w załączniku XIII, które, aby nadążyć za tempem postępu technologicznego, mogę być aktualizowane w drodze aktów delegowanych przyjmowanych przez Komisję. Zapisy regulacji nakładają na dostawców modeli AI ogólnego przeznaczenia obowiązek przestrzegania określonych standardów. Aby ułatwić zapewnienie spójności, Urząd ds. AI zachęca odpowiednie zainteresowane strony, takie jak organizacje społeczeństwa obywatelskiego, przedstawicieli przemysłu, środowisko akademickie, dostawców niższego szczebla i niezależnych ekspertów do włączenia się w proces opracowywania dodatkowych kodeksów postępowania na poziomie UE. Organizacje wykorzystujące systemy AI ogólnego przeznaczenia nie mają obowiązku stosowania kodeksów postępowania, ale jeśli to robią domniemuje się, że spełniają określone wymogi. Za opracowanie kodeksów, ich monitorowanie i ocenę odpowiada Urząd ds. AI, odbiorca raportów wdrożeniowych.

Dostawcy modeli AI, które są udostępniane na podstawie bezpłatnej licencji otwartego oprogramowania umożliwiającej dostęp, wykorzystanie, zmianę i dystrybucję modelu i których parametry są podawane do wiadomości publicznej, oraz które nie stwarzają ryzyka systemowego, są objęci obowiązkiem w ograniczonym zakresie.

Model AI ogólnego przeznaczenia oznacza model AI, w tym model AI trenowany dużą ilością danych z wykorzystaniem nadzoru własnego na dużą skalę, który wykazuje znaczną ogólność i jest w stanie kompetentnie wykonywać szeroki zakres różnych zadań, niezależnie od sposobu, w jaki model ten jest wprowadzany do obrotu, i który można zintegrować z różnymi systemami lub aplikacjami niższego szczebla.

System AI ogólnego przeznaczenia oznacza system AI oparty na modelu AI ogólnego przeznaczenia, który to system może służyć różnym celom, nadający się zarówno do bezpośredniego wykorzystania, jak i do integracji z innymi systemami AI.

Tabela 4 – Obowiązki modeli AI ogólnego przeznaczenia

Modele AI ogólnego przeznaczenia	Modele AI ogólnego przeznaczenia wykazujące zdolność dużego oddziaływania („ryzyko systemowe”)
Duże modele i systemy zdolne do kompetentnego wykonywania szerokiego zakresu różnych zadań, takich jak generowanie wideo, tekstu, obrazów, kodu komputerowego lub rozmowy	Modele podstawowe trenowane na dużej ilości danych, o zaawansowanej złożoności, dużych możliwościach i wydajności znacznie powyżej średniej, które mogą rozprzestrzeniać ryzyko systemowe w całym łańcuchu wartości
• Sporządzanie i aktualizowanie dokumentacji technicznej na potrzeby Urzędu ds. AI i organów krajowych (wymienionych w załączniku XI) oraz dostawców niższego szczebla (wymienionych w załączniku XII)	• Zapewnienie zgodności ze wszystkimi wymaganiami mającymi zastosowanie do wszystkich modeli i systemów AI ogólnego przeznaczenia
• Ochrona praw własności intelektualnej, tajemnic przedsiębiorstwa i poufnych informacji handlowych	• Przeprowadzanie ocen modeli
• Umożliwienie zrozumienia ograniczeń i możliwości modeli AI ogólnego przeznaczenia	• Dokonywanie oceny i ograniczanie ryzyk systemowych, w tym ich źródeł
• Przestrzeganie unijnego prawa autorskiego i sporządzanie szczegółowych streszczeń treści wykorzystywanych do trenowania model	• Przeprowadzanie testów kontradyktoryjnych
	• Śledzenie, dokumentowanie i zgłaszanie poważnych incydentów do Komisji Europejskiej
	• Zapewnienie odpowiedniego poziomu ochrony cyberbezpieczeństwa
	• Raportowanie efektywności energetycznej i szacowanie zużycia energii na potrzeby trenowania modeli

Obowiązkiem dostawców modeli AI ogólnego przeznaczenia udostępnianych na podstawie bezpłatnej licencji otwartego oprogramowania jest jedynie przedstawienie szczegółowych informacji na temat treści wykorzystywanych do trenowania modeli oraz przestrzeganie unijnych przepisów dotyczących praw autorskich. Natomiast w przypadku, gdy model ogólnego przeznaczenia zostanie uznany za stwarzający ryzyko systemowe, dostawy muszą spełnić wszystkie obowiązki.

6. Ład regulacyjny i egzekwowanie przepisów

Kompetencje w zakresie egzekwowania przepisów Aktu AI zostaną rozdzielone między nowo utworzony Urząd ds. AI przy Komisji Europejskiej, a organy nadzorcze w państwach członkowskich.

Pomimo różnic między zakresami obowiązków, Komisja Europejska i państwa członkowskie współpracują w celu monitorowania i egzekwowania nowych przepisów dotyczących systemów sztucznej inteligencji oraz modeli AI ogólnego przeznaczenia. Głównym obszarem odpowiedzialności Komisji jest nadzór nad modelami AI ogólnego przeznaczenia, z kolei organy państw członkowskich zajmują się egzekwowaniem przepisów dotyczących systemów AI opartych na analizie ryzyka oraz koordynowaniem piaskownic regulacyjnych na szczeblu loklanym. Poniższy rozdział zawiera informacje na temat konkretnych obowiązków, struktury zarządzania i wzajemnych powiązań między Komisją Europejską a państwami członkowskimi.

6.1 Szczebel krajowy – egzekwowanie przepisów przez państwa członkowskie

Państwa członkowskie tworzą organ nadzoru rynku, którego głównym zadaniem jest egzekwowanie przepisów Aktu AI na szczeblu krajowym.

Organy nadzoru rynku są odpowiedzialne za zapewnienie, aby systemy sztucznej inteligencji były zgodne z określonymi normami i przepisami. Na przykład: zadaniem organu nadzoru rynku jest nadzorowanie prawidłowości oceny zgodności przeprowadzanej przez dostawców modeli AI wysokiego ryzyka. W trakcie postępowań organy nadzoru rynku mogą podejmować niezbędne działania, w tym wystąpić o uzyskanie dostępu do dokumentacji oraz zbiorów danych treningowych, walidacyjnych i testowych wykorzystywanych do opracowywania systemów AI wysokiego ryzyka, jak również dostępu do kodu źródłowego systemów AI wysokiego ryzyka. Dostawcy systemów AI wysokiego ryzyka są zobowiązani do współpracy z organami.

Organ notyfikujący jest odpowiedzialny za wyznaczenie jednostek oceniających zgodność, które po prawidłowym zgłoszeniu mogą zostać zakwalifikowane jako jednostki notyfikowane (zob. rozdział 4). W tym celu konieczne jest spełnienie kilku warunków, w tym posiadanie osobowości prawnej na mocy prawa krajowego, spełnianie wymogów organizacyjnych dot. powierzanych zadań oraz niezależność od dostawców systemów AI wysokiego ryzyka.

Ponadto, rolą każdego państwa członkowskiego będzie przypisanie konkretnych obowiązków i nadanie uprawnień istniejącym lub nowo utworzonym organom odpowiedzialnym za ochronę praw podstawowych w zakresie sztucznej inteligencji. Właściwe organy powinny wykonywać swoje uprawnienia w w sposób niezależny i bezstronny, aby zapewnić przestrzeganie praw podstawowych przez organizacje na etapie opracowywania, wdrażania i wykorzystywania systemów AI.

6.2 Szczebel europejski – egzekwowanie przepisów przez Unię Europejską

Z myślą o usprawnieniu procesu wdrażania Aktu AI oraz zapewnieniu odpowiedniego nadzoru, w lutym 2023 r. Unia Europejska ustanowiła Urząd ds. AI, nowy podmiot powołany przez Komisję Europejską. Odgrywa ona kluczową rolę we wdrażaniu nowych przepisów. Urząd ds. AI ustanowiono w ramach struktury administracyjnej Dyrekcji Generalnej ds. Sieci Komunikacyjnych, Treści i Technologii, dzięki czemu dysponuje on większą swobodą w zakresie decyzyjności oraz może działać w bardziej dynamiczny sposób. W skład Urzędu będzie wchodzić pięć głównych departamentów. Każdy z nich będzie zarządzany przez dyrektora odpowiedzialnego za nadzór nad wdrażaniem Aktu AI. Urząd ds. AI zatrudni łącznie 140 osób, w tym ekspertów z obszaru technologii, prawników i specjalistów ds. polityki. Obecnie prace Urzędu skupiają się na wdrożeniu regulacji i obejmują ponad 50 zadań.

W Akcie AI wymieniono szereg aspektów, które będą podlegały dalszemu wdrażaniu przez Urząd ds. AI w drodze aktów delegowanych i wykonawczych. Obecnie regulacja ma charakter bardzo teoretyczny i wymaga doprecyzowania.

Akty delegowane służą uzupełnieniu lub zmianie elementów aktu ustawodawczego, natomiast akty wykonawcze określają szczegółowe zasady wykonywania aktu, mogę mieć zasięg ogólny lub indywidualny. Na przykład Urząd ds. AI może zmienić wykaz zawarty w każdym załączniku do Aktu AI w drodze aktu delegowanego.

Kolejnym, wymagającym zadaniem stojącym przed Urzędem, biorąc pod uwagę harmonogram wdrożenia, jest opracowanie konkretnych przykładów zakazanych i dozwolonych praktyk AI. Tego rodzaju działania mają na celu zapewnienie skutecznego wdrożenia regulacji oraz doprecyzowanie zasad i pojęć określonych w jej treści.

Oprócz tego, Urząd ds. AI będzie odpowiedzialny za egzekwowanie obowiązków wynikających z Aktu w sprawie sztucznej inteligencji w odniesieniu do modeli AI ogólnego przeznaczenia. W tym celu, we współpracy z przedstawicielami środowiska akademickiego i przemysłu, zostaną opracowane narzędzia projektowe, metodologie i punkty odniesienia, aby móc ocenić możliwości i zasięg modeli AI ogólnego przeznaczenia oraz wyodrębnić modele stwarzające ryzyko systemowe. Poza wymienionymi obowiązkami, Urząd ds. AI będzie również prowadził publiczny rejestr zawierający wykaz wszystkich zastosowań AI wysokiego ryzyka funkcjonujących na rynku.

Oprócz Urzędu ds. AI istnieją jeszcze dwa organy UE, które również będą miały wpływ na egzekwowanie postanowień nowej regulacji. Pierwszy z nich to Forum Doradcze, którego zadaniem będzie zacieśnienie współpracy między zainteresowanymi stronami oraz zapewnienie kompleksowych wytycznych dot. Aktu AI.

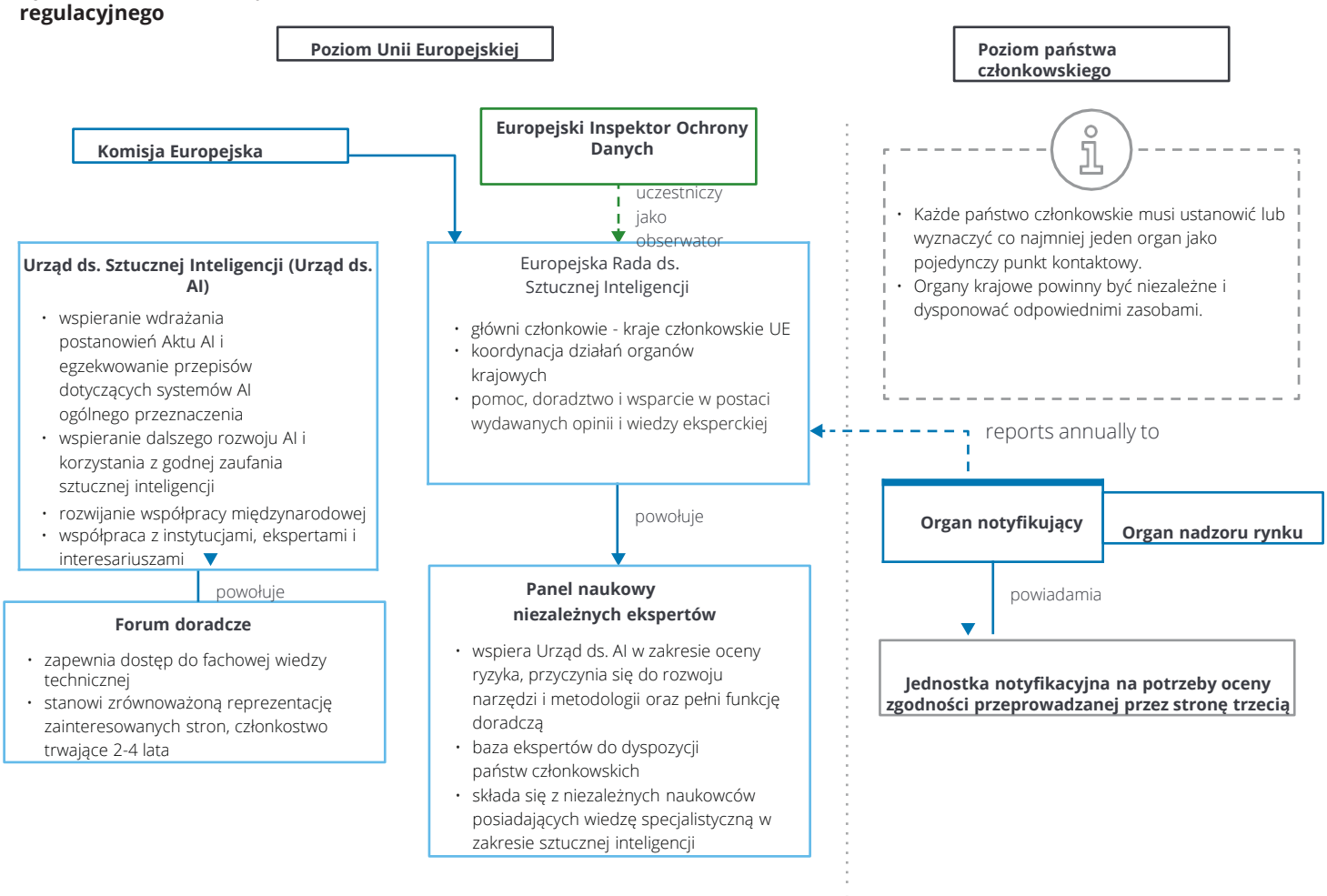
W skład Forum wchodzi szereg zainteresowanych stron - eksperci branżowi, przedstawiciele społeczeństwa obywatelskiego, badacze i urzędnicy państwowi. Członkowie Forum Doradczego, powołani przez Komisję Europejską, wpierają proces wdrażania Aktu AI, oferując swoją fachową wiedzę techniczną i perspektywę strategiczną. Drugim organem jest Panel naukowy niezależnych ekspertów, który ma za zadanie doradzanie Komisji i informowanie o wystąpieniu ryzyka systemowego związanego ze stosowaniem systemów AI ogólnego przeznaczenia.

6.3 Egzekwowanie przepisów na szczeblu europejskim i krajowym

Europejska Rada ds. Sztucznej Inteligencji, składająca się z przedstawicieli każdego państwa członkowskiego, a także obserwatorów, takich jak Europejski Inspektor Ochrony Danych i Urząd ds. AI, współpracuje z odpowiednimi zainteresowanymi stronami w celu zapewnienia spójnego i skutecznego stosowania rozporządzenia. Rada, której powierzono różnorodne zadania - od koordynowania pracy właściwych organów krajowych po wydawanie zaleceń w kwestiach regulacyjnych, odgrywa kluczową rolę przy rozwijaniu współpracy, dzieleniu się wiedzą specjalistyczną i promowaniu dobrego zrozumienia sztucznej inteligencji w całej UE.

Ponadto, aby móc skutecznie stawić czoła wszystkim istotnym wyzwaniom związanym z Aktem w sprawie sztucznej inteligencji, Rada zostanie podzielona na różne podkomitety, których zadaniem będzie np. dostosowanie ustawodawstwa sektorowego lub krajowego. Należy oczekiwać, że jednostki notyfikujące i organy nadzoru rynku poszczególnych państw członkowskich będą uczestniczyć w posiedzeniach podkomitetów i reprezentować interesy swoich krajów.

Rys. 6 – Struktura zarządzania regulacyjnego



7. Akt w sprawie sztucznej inteligencji i udogodnienia w zakresie przeprowadzania testów w środowisku testowym (tzw. sandbox testing)

Państwa członkowskie są upoważnione do ustanowienia piaskownic regulacyjnych w zakresie sztucznej inteligencji na szczeblu krajowym w ciągu 24 miesięcy od daty wejścia rozporządzenia w życie, czyli w III kw. 2026 r. Jednocześnie mogą ustanowić wspólną piaskownicę lub uczestniczyć w już istniejących piaskownicach regulacyjnych. Głównym celem jest zapewnienie wszystkim przedsiębiorstwom z siedzibą w UE możliwości uczestnictwa w piaskownicy regulacyjnej, czyli zagwarantowanie równego dostępu i równoważnego poziomu zasięgu krajowego dla uczestniczących państw członkowskich. Ponadto, możliwe jest ustanowienie piaskownic na poziomie regionalnym lub lokalnym. W związku z tym oczekuje się, że większe państwa utworzą kilka piaskownic, aby zapewnić małym i średnim przedsiębiorstwom wsparcie na szczeblu regionalnym lub lokalnym. Dodatkowo, Europejski Inspektor Ochrony Danych może ustanowić piaskownicę regulacyjną w zakresie AI na szczeblu Unii Europejskiej.

7.1 Piaskownice regulacyjne w zakresie AI

Piaskownice regulacyjne w zakresie AI to kontrolowane środowiska, w których operatorzy systemów sztucznej inteligencji mają możliwość rozwoju, trenowania, testowania i walidacji swoich systemów AI przed wdrożeniem ich na rynek. Oferują one bezpieczną przestrzeń do eksperymentowania, pozwalając na eksplorację zastosowań sztucznej inteligencji pod nadzorem kompetentnych organów. Wprowadzenie piaskownic regulacyjnych jest pionierskim projektem, wspierającym innowacyjność w ramach UE. Jego zadaniem jest zapewnienie kontrolowanego środowiska, które ułatwi rozwój oraz testowanie systemów sztucznej inteligencji. Z kolei rolą właściwych organów krajowych jest zapewnienie odpowiednich zasobów, aby spełnić wymogi określone w Akcie AI, oraz przedkładanie Urzędowi ds. AI sprawozdań rocznych zawierających opis postępów wdrażania piaskownic, w tym informacje dot. najlepszych praktyk, incydentów, wyciągniętych wniosków i rekomendacji.

Do piaskownicy mogą dołączyć zarówno podmioty publiczne, jak i prywatne, które chcą przetestować swoje systemy AI. Wystarczy złożyć wniosek.
Po przystąpieniu do piaskownicy podmioty otrzymują realne wsparcie i wskazówki w zakresie identyfikowania ryzyka w zakresie praw podstawowych, zdrowia i bezpieczeństwa, podlegają też nadzorowi. Na zakończenie każdy uczestnik otrzymuje sprawozdanie końcowe zawierające szczegółowe informacje na temat działań przeprowadzonych w piaskownicy, powiązanych rezultatów i efektów uczenia się. Dostawcy mogą wykorzystać dokumentację do wykazania swojej zgodności z rozporządzeniem w ramach procesu oceny zgodności (domniemania zgodności), co z pewnością uznają za niewątpliwy atut.

W świecie sztucznej inteligencji piaskownice regulacyjne są katalizatorami innowacji, oferując ustrukturyzowane i wspierające środowisko do opracowywania i testowania systemów AI przy zapewnieniu zgodności z normami regulacyjnymi. Co istotne, sprawozdania końcowe, które uczestnicy piaskownic otrzymają na zakończenie całego procesu, posłużą jako domniemanie zgodności na potrzeby niezbędnej oceny zgodności systemów AI wysokiego ryzyka.

7.1.1 Testowanie systemów AI wysokiego ryzyka w warunkach rzeczywistych, bez udziału w piaskownicy regulacyjnej

Podczas gdy piaskownice regulacyjne oferują kontrolowane środowiska do wstępnego testowania i walidacji, testy w warunkach rzeczywistych są ich uzupełnieniem, zapewniając wgląd w faktyczną wydajność, użyteczność i opinie użytkowników, co ostatecznie przyczynia się do odpowiedzialnego i skutecznego wdrażania technologii AI.

Przeprowadzanie testów systemów AI w warunkach rzeczywistych, poza piaskownicami regulacyjnymi, daje dostawcom możliwość testowania systemów AI wysokiego ryzyka wymienionych w załączniku III.

Warto dodać, że testy należy przeprowadzać zgodnie ze szczegółowym planem testów w warunkach rzeczywistych, zatwierdzonym przez organy nadzoru rynku. Dostawcy muszą zapewnić zgodność z prawem unijnym i krajowym, nie zapominając o kwestiach etycznych. Testy mogą być przeprowadzane niezależnie lub we współpracy z potencjalnymi stosującymi, za świadomą zgodą uczestników. Ponadto, czas trwania testów, ochrona danych, nadzór i odwracalność decyzji systemu AI podlegają rygorystycznym zasadom; a wszelkie incydenty należy niezwłocznie zgłaszać organom nadzoru rynku.

Przed rozpoczęciem testowania przy użyciu danych osób fizycznych niezbędne jest uzyskanie świadomej zgody uczestników po uprzednim poinformowaniu ich o charakterze testów, ich celu, czasie trwania i przysługującym im prawach, oraz udostępnienie im danych kontaktowych w razie dalszych zapytań. Warto również podkreślić, że odpowiedzialność za szkody powstałe w wyniki działalności testowej ponoszą dostawcy.

7.2 Działania wspierające MŚP i przedsiębiorstwa typu start-up w spełnianiu norm określonych w rozporządzeniu

Akt w sprawie sztucznej inteligencji ma na celu uproszczenie niektórych aspektów wymogów regulacyjnych dla małych i średnich przedsiębiorstw (MŚP) oraz przedsiębiorstw typu start-up. Zadaniem państw członkowskich jest podjęcie działań, które pomogą MŚP i start-upom w odnalezieniu się w nowym otoczeniu regulacyjnym, w tym zapewnienie im dostępu do piaskownic regulacyjnych w zakresie AI na zasadzie pierwszeństwa, organizowanie wydarzeń informacyjnych i szkoleniowych poświęconych stosowaniu przepisów rozporządzenia dostosowanych do potrzeb MŚP, ustanowienie kanałów komunikacyjnych w celu zapewnienia poradnictwa i udzielania odpowiedzi na zapytania, a także ułatwienie im udziału w procesie opracowywanie norm.

Natomiast kary przewidziane za naruszenie przepisów są ustalane proporcjonalnie, w oparciu o konkretne czynniki, takie jak wielkość i pozycja rynkowa MŚP i przedsiębiorstw typu start-up.

Nie bez znaczenia jest też rola Urzędu ds. AI, którego działania obejmują m.in. zapewnienie ujednoliconych wzorów formularzy, obsługę platformy informacyjnej, organizację kampanii informacyjnych oraz promowanie najlepszych praktyki w postępowaniach o udzielenie zamówienia publicznego w odniesieniu do systemów AI. Celem tych działań jest wzmocnienie pozycji MŚP i przedsiębiorstw typu start-up oraz udzielenie wsparcia w zakresie przestrzegania przepisów i rozwoju w ekosystemie AI.

8. Wysokie kary za nieprzestrzeganie przepisów – o wiele wyższe niż w przypadku RODO

System kar przewidziany w Akcie AI jest skonstruowany w oparciu o charakter naruszenia. Przy ustalaniu wysokości kary uwzględnia się istotne okoliczności danego naruszenia, np. czy stwarza niedopuszczalne ryzyko, czy jest związane ze stosowaniem modeli AI wysokiego ryzyka czy też modeli AI ogólnego przeznaczenia. Innymi słowy, im wyższa kategoria ryzyka danego naruszenia, tym wyższa kwota kary pieniężnej.

Odpowiedzialność za ustanowienie przepisów dotyczących kar i innych środków egzekwowania prawa ponoszą państwa członkowskie. Na przykład: każde państwo członkowskie ma swobodę decydowania o stosowaniu ostrzeżeń i innych środków niepieniężnych, jeśli takie mają zastosowanie. Co więcej, muszą mieć na uwadze szczególne interesy MŚP i przedsiębiorstw typu start-up. Organy krajowe są również upoważnione do oceny charakteru, wagi i czasu trwania naruszenia; przy ustalaniu wysokości kary uwzględnia się również wszelkie podobne wcześniejsze naruszenia dokonane przez dany podmiot.

Oprócz kar pieniężnych, krajowe organy nadzoru mogą zdecydować o przymusowym usunięciu z rynku systemów AI niespełniających wymogów.

Rys. 7 – Kary dla operatorów systemów AI

1. Kara za nieprzestrzeganie zakazów: do 35 mln EUR lub – jeżeli sprawcą naruszenia jest przedsiębiorstwo – do 7% całkowitego rocznego światowego obrotu

2. Kara za naruszenie przepisów dot. systemów AI wysokiego ryzyka: do 15 mln EUR lub – jeżeli sprawcą naruszenia jest przedsiębiorstwo – do 3% jego całkowitego rocznego światowego obrotu

3. Kara za naruszenie przepisów dot. systemów AI ogólnego przeznaczenia: do 15 mln EUR lub – jeżeli sprawcą naruszenia jest przedsiębiorstwo – do 3% jego całkowitego rocznego światowego obrotu

4. Kara za dostarczanie nieprawidłowych, niekompletnych lub wprowadzających w błąd informacji: do 7,5 mln EUR lub – jeżeli sprawcą naruszenia jest przedsiębiorstwo – w wysokości do 1% jego całkowitego rocznego światowego obrotu

9. Stopniowe wprowadzanie Aktu w sprawie sztucznej inteligencji w życie

Unijny Akt w sprawie sztucznej inteligencji wchodzi w życie dwadzieścia dni po jego opublikowaniu w Dzienniku Urzędowym UE tj. 1 sierpnia 2024 r. Wtedy też rozpoczyna się oficjalne wdrażanie jego postanowień. Co istotne, nie wszystkie przepisy zaczną obowiązywać w tym samym czasie. Niektóre z nich wymagają podjęcia natychmiastowych działań, podczas gdy inne dają operatorom więcej czasu na dostosowanie się do ustalonych wymogów.

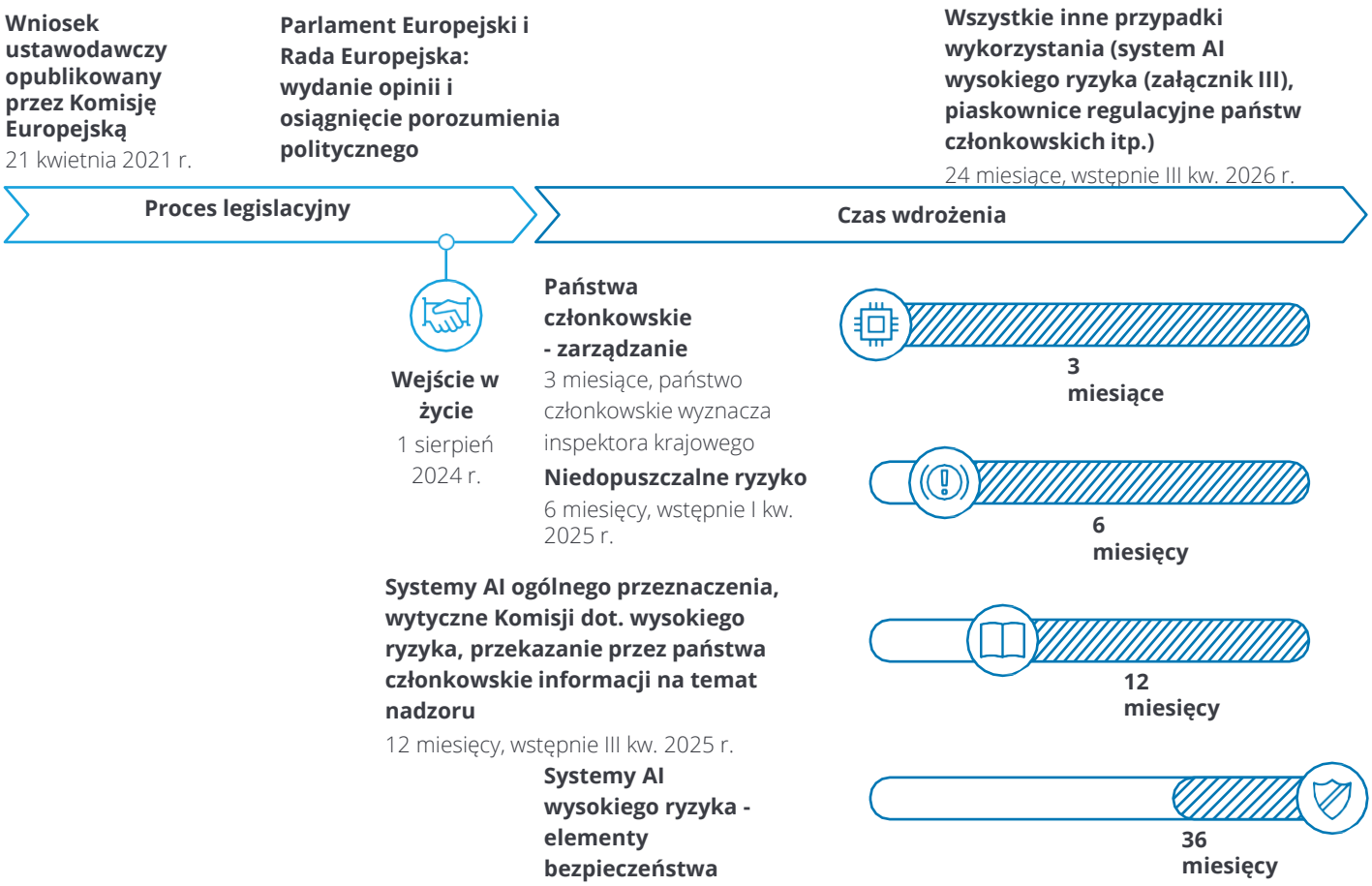
Większość przepisów ma zacząć obowiązywać po upływie 24 miesięcy, z pewnymi wyjątkami: przepisy dot. zakazanych praktyk wejdą w życie po sześciu miesiącach, natomiast zasady zarządzania i obowiązki dotyczące modeli sztucznej inteligencji ogólnego przeznaczenia zaczną obowiązywać po 12 miesiącach.

Z kolei zasady dotyczące systemów sztucznej inteligencji – wbudowanych w produkty regulowane – zaczną obowiązywać po 36 miesiącach. Na poniższym rysunku przedstawiono harmonogram wdrażania poszczególnych przepisów istotnych z perspektywy operatorów funkcjonujących na rynku UE.

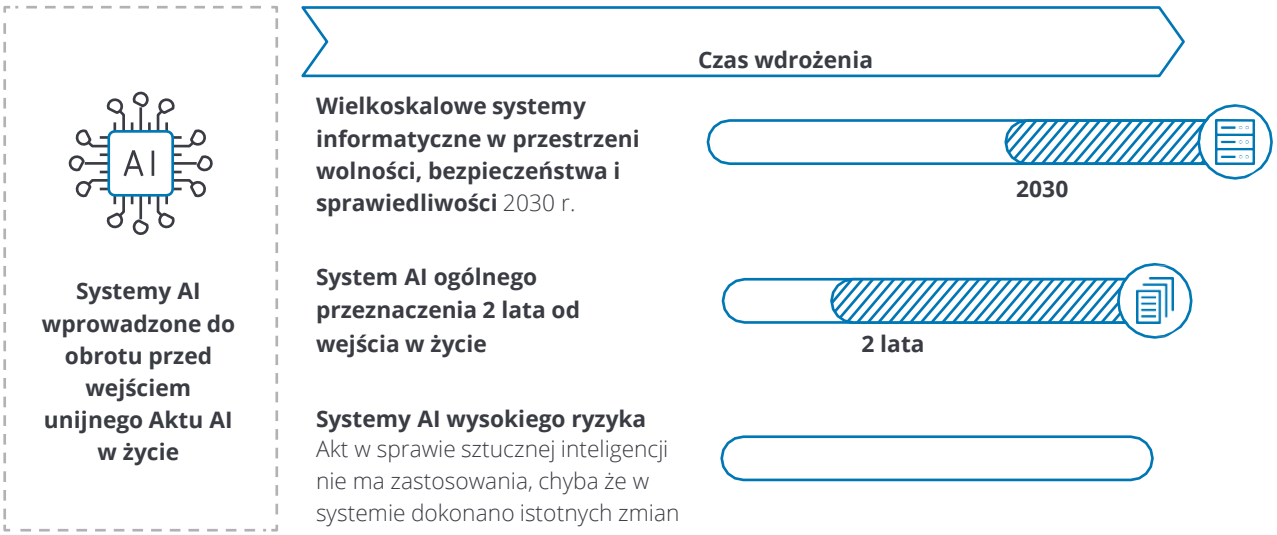
Nowe postanowienia nie maja zastosowania do systemów AI, które zostały wprowadzone do obrotu na rynku unijnym przed wejściem Aktu AI w życie lub wkrótce po jego wejściu w życie; nie stosuje się też wobec nich przedłużonego okresu wdrożenia (rys. 9).

W związku z tym operatorzy systemów AI ogólnego przeznaczenia, które zostały wprowadzone do obrotu przed wejściem Aktu AI w życie lub w ciągu pierwszych 12 miesięcy po jego wejściu w życie, mają 36 miesięcy na wdrożenie nowych wymogów unijnych. Natomiast systemy AI wysokiego ryzyka wprowadzone do obrotu przed wejściem rozporządzenia w życie lub w ciągu pierwszych 24 miesięcy po jego wejściu w życie, nie będą automatycznie podlegać przepisom Aktu AI, chyba że wprowadzone do nich zostaną „istotne zmiany". Wówczas będą musiały spełniać wymogi określone w rozporządzeniu. Przy czym jeszcze nie wiadomo, co przesądzi o przypisaniu zmian do kategorii „istotne" oraz jak rygorystycznie Komisja będzie stosować tę zasadę.

Rys. 8 – Harmonogram wdrożenia postanowień Aktu w sprawie sztucznej inteligencji



Rys. 9 – Harmonogram wdrożenia Aktu w sprawie sztucznej inteligencji - szczególne przypadki



Całkiem niedawno Komisja Europejska zainicjowała pakt na rzecz sztucznej inteligencji. Jest to inicjatywa, której celem jest zachęcenie organizacji do przyjęcia dobrowolnego zobowiązania, polegającego na przestrzeganiu postanowień Aktu w sprawie sztucznej inteligencji jeszcze przed jego oficjalnym wejściem w życie w II kwartale 2026 r. Pakt ma stanowić platformę współpracy, która umożliwi przedsiębiorstwom wymianę pomysłów i dobrych praktyk w zakresie stosowania się do nowych wytycznych. Obecnie Komisja bada zainteresowanie inicjatywą wśród biznesu. Wstępne spotkanie dla zainteresowanych stron zaplanowano na początek lub połowę 2024 r. Przynależąc do paktu, firmy zobowiązują się do przestrzegania przepisów Aktu w sprawie sztucznej inteligencji oraz przedstawienia działań, jakie podejmują w celu zapewnienia zgodności. Wszystkie zgłoszone pomysły zostaną zebrane i udostępnione szerszej grupie odbiorców.

Rolą Komisji jest udzielenie firmom wsparcia w zakresie zrozumienia zapisów Aktu w sprawie sztucznej inteligencji, zapewnienie pomocy na etapie przygotowania i dostosowania się do nowych regulacji, promowanie wymiany wiedzy oraz zwiększanie zaufania do technologii AI.

Ponadto, Europejski Komitet Normalizacyjny (CEN) wraz z Europejskim Komitetem Normalizacyjnym Elektrotechniki (CENELEC) rozpoczął proces wdrażania Aktu w sprawie sztucznej inteligencji za pomocą norm.

Firmy, które już stosują lub zamierzają wykorzystywać systemy AI w swojej działalności muszą zapewnić zgodność z wymogami w określonym terminie. W tym celu niezbędne jest opracowanie planu wdrożenia oraz szybkie podjęcie działań.

.

Nawet jeśli nie wszystkie szczegóły techniczne zostały dostatecznie wyjaśnione, Akt w sprawie sztucznej inteligencji daje wyobrażenie o zakresie i celu przyszłego rozporządzenia. Jedno jest pewne, przedsiębiorstwa będą musiały zmodyfikować wiele swoich procesów wewnętrznych oraz wzmocnić systemy zarządzania ryzykiem. Tutaj pomocne może okazać się doświadczenie zdobyte przy okazji wdrażania innej ważnej regulacji unijnej - RODO. W naszej ocenie nie należy zwlekać. Firmy już teraz powinny zacząć przygotowywać się na przyjęcie nowych przepisów oraz poinformować pracowników o nadchodzących zmianach regulacyjnych. Warto dokonać przeglądu stosowanych systemów AI, opracować plan działania, wprowadzić odpowiednią klasyfikację ryzyka i system zarządzania ryzykiem w odniesieniu do AI oraz dokładnie przyjrzeć się systemom AI należącym do kategorii wysokiego ryzyka.

10. Glosariusz

Terminologia zaczerpnięta z Aktu w sprawie sztucznej inteligencji

Dostawca: oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które rozwijają system AI lub model AI ogólnego przeznaczenia lub zlecają rozwój systemu AI lub modelu AI ogólnego przeznaczenia oraz które – odpłatnie lub nieodpłatnie – pod własną nazwą lub własnym znakiem towarowym wprowadzają do obrotu lub oddają do użytku system AI;

Dostawca niższego szczebla: oznacza dostawcę systemu AI, w tym systemu AI ogólnego przeznaczenia, rozwiniętego w drodze integracji modelu AI, niezależnie od tego, czy ten model AI jest dostarczany przez tego samego dostawcę i zintegrowany pionowo czy dostarczany przez inny podmiot na podstawie stosunków umownych.

Podmiot stosujący: oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które wykorzystują system AI, nad którym sprawują kontrolę, z wyjątkiem sytuacji, gdy system AI jest wykorzystywany w ramach osobistej działalności pozazawodowej;

Upoważniony przedstawiciel: oznacza osobę fizyczną lub prawną znajdującą się lub mającą siedzibę w Unii, która otrzymała i przyjęła pisemne pełnomocnictwo od dostawcy systemu AI lub modelu AI ogólnego przeznaczenia do, odpowiednio, spełnienia w jego imieniu obowiązków i przeprowadzania procedur ustanowionych w niniejszym rozporządzeniu;

Importer: oznacza osobę fizyczną lub prawną znajdującą się lub mającą siedzibę w Unii, która wprowadza do obrotu system AI opatrzony nazwą lub znakiem towarowym osoby fizycznej lub prawnej mającej siedzibę w państwie trzecim;

Dystrybutor: oznacza osobę fizyczną lub prawną w łańcuchu dostaw, inną niż dostawca lub importer, która udostępnia system AI na rynku Unii;

Operator: oznacza dostawcę, producenta produktu, podmiot stosujący, upoważnionego przedstawiciela, importera lub dystrybutora;

Dane biometryczne: oznaczają dane osobowe będące wynikiem specjalnego przetwarzania technicznego, które dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej, takich jak wizerunek twarzy lub dane daktyloskopijne;

Identyfikacja biometryczna: oznacza zautomatyzowane rozpoznawanie fizycznych, fizjologicznych, behawioralnych lub psychologicznych cech ludzkich w celu ustalenia tożsamości osoby fizycznej przez porównanie danych biometrycznych tej osoby z danymi biometrycznymi osób fizycznych przechowywanymi w bazie danych;

Weryfikacja biometryczna: oznacza zautomatyzowaną weryfikację typu jeden-do-jednego, w tym uwierzytelnianie, tożsamości osób fizycznych przez porównanie ich danych biometrycznych z wcześniej przekazanymi danymi biometrycznymi;

System rozpoznawania emocji: oznacza system AI służący do identyfikacji lub wywnioskowania emocji lub zamiarów osób fizycznych na podstawie danych biometrycznych tych osób;

System kategoryzacji biometrycznej: oznacza system AI służący do przypisywania osób fizycznych do określonych kategorii na podstawie danych biometrycznych tych osób, oprócz przypadków, gdy taki system pełni funkcję pomocniczą w stosunku do innej usługi komercyjnej i jest bezwzględnie konieczny z obiektywnych względów technicznych;
to another commercial service and strictly necessary for objective technical reasons.

System zdalnej identyfikacji biometrycznej: oznacza system AI służący do identyfikacji osób fizycznych bez ich aktywnego udziału, zwykle na odległość, poprzez porównanie danych biometrycznych danej osoby fizycznej z danymi biometrycznymi zawartymi w referencyjnej bazie danych;

System zdalnej identyfikacji biometrycznej w czasie rzeczywistym: oznacza system zdalnej identyfikacji biometrycznej, w którym zbieranie danych biometrycznych, ich porównywanie i identyfikacja odbywają się bez znacznego opóźnienia, i który obejmuje nie tylko natychmiastową identyfikację, ale także ograniczone krótkie opóźnienia w celu uniknięcia obchodzenia przepisów;

Deep fake: oznacza wygenerowane przez AI lub zmanipulowane przez AI obrazy, treści dźwiękowe lub treści wideo, które przypominają istniejące osoby, przedmioty, miejsca, podmioty lub zdarzenia, które odbiorca mógłby niesłusznie uznać za autentyczne lub prawdziwe;

Czekamy na kontakt z Państwa strony

Zachęcamy do kontaktu! Z przyjemnością opowiemy o nowych przepisach i zaproponujemy wsparcie w zakresie AI.

EUROPA ŚRODKOWA

Jan Michalski
Partner,
Central Europe GenAI Leader
jmichalski@deloittece.com

Simina Mut
Partner,
Deloitte Legal Central Europe Leader
smut@deloittece.com

Gregor Strojin
Deloitte Legal Central Europe
AI Regulatory CoE Leader
gstrojin@deloittece.com

ALBANIA

Ina Cota
Manager
icota@deloittece.com

Ened Topi
Senior Manager,
Deloitte Legal
etopi@deloittece.com

BOŚNIA i HERCEGOWINA

Elma Delalic-Haskovic
Manager
edelalic@deloittece.com

Zerina Pacariz
Manager
zpacariz@deloittece.com

BUŁGARIA

Mila Goranova
Senior Consultant
mgoranova@deloittece.com

Adelina Mitkova
Senior Manager,
Deloitte Legal
amitkova@deloittece.com

CHORWACJA

Zrinka Vrtarić
Attorney at law
in cooperation
with Deloitte Legal
zvrtaric@kip-legal.hr

Ratko Drča
Director
rdrca@deloittece.com

CZECHY

Jaroslava Kracunova
Partner,
Deloitte Legal
jkracunova@deloittece.com

Jakub Holl
Director
jholl@deloittece.com

ESTONIA, ŁOTWA, LITWA

Maksims Naumovs
Data Modernization
and Analytics Offering
Lead at Deloitte Central
Europe,
AI & Data Director
mnaumovs@deloittece.com

Romans Taranovs
AI & Data Director
rtaranovs@deloittece.com

WĘGRY

dr. Lili Albert LL.M.
Senior Associate,
Deloitte Legal
lialbert@deloittece.com

Gergő Barta, Ph.D.
Senior Manager
AI Risk & Compliance
gbarta@deloittece.com

KOSOWO

Donika Ahmeti
Senior Manager
dahmeti@deloittece.com

Ardian Rexha
Senior Manager
Deloitte Legal

POLSKA

Mateusz Ordyk
Partner,
Deloitte Legal
mordyk@deloittece.com

Scibor Lapies
Partner
slapies@deloittece.com

RUMUNIA

Simina Mut
Partner,
Deloitte Legal
Central Europe Leader
smut@deloittece.com

Andrei Paraschiv
Partner
anparaschiv@deloittece.com

SERBIA

Stefan Ivic
Partner
stivic@deloittece.com

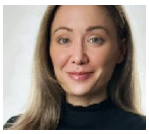
Miroslava Gaćeša
Dyrektor
mgacesa@deloitteCE.com

SŁOWACJA

Dagmar Yoder
Partner,
Deloitte Legal
dyoder@deloittece.com

Pavol Szabo
Senior Managing
Associate,
Deloitte Legal
pszabo@deloittece.com

SŁOWENIA

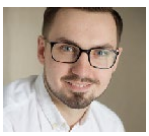


Ana Kastelec, LL.M.
Radca prawny, Local Partner
in Law Firm Deloitte Legal
Reff – oddział na Słowenii
akastelec@deloittece.com

Lan Filipič
Director
lfilipic@deloittece.com

UKRAINA

Andrii Krasnyi
Dyrektorakrasnyi@deloit
tece.com



Vadym Matuzenko
Senior Manager
vmatuzenko@deloittece.com

Autorzy

Dr. Till Contzen
Partner | Legal
Intangibles, Data & Technology
(Head for Germany)
Deloitte Legal Germany

David Thogmartin
Partner | Risk Advisory
aiStudio | AI & Data Analytics
Deloitte Germany

Torsten Berge
Dyrektor
Algorithm & AI Assurance Lead DE
Deloitte Germany

Mosche Orth
Manager
Deloitte EU Policy Centre

Zoe Marie Lohoff
Algorithm Assurance
Deloitte Germany

Deloitte.

06/2024