AMERYKAŃSKA IZBA HANDLOWA W POLSCE
Spektrum Tower, ul. Twarda 18, 00-105 Warszawa
Tel: (48) (22) 520-5999, e-mail

Warszawa, dnia 24 lutego 2025 r.

Pan Dariusz Standerski
Sekretarz Stanu w Ministerstwie Cyfryzacji

Szanowny Panie Ministrze,

w imieniu Amerykańskiej Izby Handlowej w Polsce (AmCham) oraz jej firm członkowskich dziękuję za zaproszenie do wzięcia udziału w ponownych konsultacjach publicznych projektu ustawy o systemach sztucznej inteligencji (dalej: Projekt), umożliwiającej stosowanie w polskim porządku prawnym unijnego aktu o sztucznej inteligencji[1] (dalej: Akt o AI).

AmCham jest organizacją zrzeszającą przedsiębiorców amerykańskich w naszym kraju, reprezentujących jednocześnie jedną z największych grup inwestorów zagranicznych, którzy stworzyli aktywa w Polsce o wartości 239 mld złotych i kreują 327 tysięcy miejsc pracy. Od ponad 30 lat działamy na rzecz rozwoju wzajemnych relacji gospodarczych, a naszą misją jest poprawa klimatu inwestycyjnego i promocja naszego kraju na rynku amerykańskim. W szczególności członkami AmCham są wszyscy najwięksi dostawcy sprzętu ICT oraz usług cyfrowych pochodzący ze Stanów Zjednoczonych działający w Polsce, którzy w wielu segmentach tego rynku dostarczają najwyższej jakości produkty umożliwiające szybki postęp cyfrowej transformacji naszego kraju.

AmCham docenia otwartość ministerstwa na dialog z sektorem prywatnym przejawiającą się w uwzględnieniu istotnej części uwag zgłaszanych przez organizacje zrzeszające przedsiębiorców działających w sektorze sztucznej inteligencji, jak również skierowaniu Projektu do ponownych konsultacji publicznych. Raz jeszcze wyrażamy również aprobatę wobec szybkiego podjęcia prac nad krajowym systemem stosowania norm wprowadzonych przez Akt o AI, dzięki czemu polskie rozwiązania w tej dziedzinie zyskują szczególne znaczenie w kształtowaniu się europejskich standardów stosowania Aktu o AI.

W tabeli stanowiącej załącznik do ninejszego pisma przedstawiamy uwagi firm członkowskich AmCham dotyczące nowej wersji Projektu skierowanej do powtórnych konsultacji publicznych.

Dziękując za możliwość wzięcia udziału w konsultacjach i przekazania stanowiska AmCham, deklarujemy dalszą gotowość do udziału w procesie legislacyjnym. Z uwagi na zakres i kompleksowość uwag przedstawionych w naszym stanowisku, jak również centralną rolę członków AmCham na rynku rozwiązań opartych na sztucznej inteligencji, bylibyśmy zobowiązani za możliwość spotkania z Panem Ministrem w celu omówienia postulowanych przez nas zmian w Projekcie. Osobą do kontaktu jest Marta Pawlak, Dyrektor ds. prawnych i polityk publicznych, z którą można się skontaktować pod adresem: marta.pawlak@amcham.pl oraz numerem tel.: +48 660 492 526.

Z poważaniem

Marta Pawlak, dyrektorka ds. prawnych i polityk publicznych

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).

Amerykańska Izba Handlowa w Polsce (AmCham)

Uwagi do projektu ustawy o systemach sztucznej inteligencji (UC71) **(projekt z dnia 10.02.2025 r.)**		
Podmiot zgłaszający uwagę	**Jednostka redakcyjna** **lub strona uzasadnienia** **lub pkt OSR**	**Treść uwagi/propozycja przepisu**
Uwagi do projektu ustawy		
AmCham	art. 2	Zakres terytorialny stosowania art. 2 jest niejasny. Brak wyraźnego ograniczenia zakresu stosowania ustawy do podmiotów mających siedzibę w Polsce mógłby potencjalnie umożliwić polskim władzom sprawowanie jurysdykcji nad spółkami zagranicznymi nawet jeśli nie są one fizycznie obecne w Polsce. Pomimo pewnych ulepszeń w stosunku do poprzedniej wersji, niejednoznaczne sformułowanie projektu dotyczące stosowania terytorialnego może prowadzić do nakładania się przepisów i potencjalnych konfliktów z mechanizmami współpracy transgranicznej określonymi w Akcie o AI. Aby ograniczyć to ryzyko, projekt powinien wyraźnie stwierdzać, że ma on zastosowanie wyłącznie do spółek z siedzibą w Polsce, co jest zgodne zarówno z polskim prawem gospodarczym, jak i ramami Aktu o AI w zakresie nadzoru transgranicznego.
AmCham	art. 2 ust. 2	Stwierdzenie zawarte w art. 2 ust. 2 dotyczące modeli sztucznej inteligencji ogólnego przeznaczenia powoduje niepotrzebne zamieszanie i należy je usunąć lub doprecyzować, aby uniknąć łączenia wymogów dotyczących modeli GPAI i systemów sztucznej inteligencji wysokiego ryzyka. Akt o AI

		stanowi, że Biuro AI/Komisja UE ma władzę regulacyjną nad modelami GPAI – państwa członkowskie nie tworzą i nie powinny tworzyć dodatkowych wymagań dla modeli GPAI na mocy przepisów wykonawczych.
AmCham	art. 5	Jest: Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji Propozycja: Komisja nadzoru nad stosowaniem systemów sztucznej inteligencji lub inna oddająca rzeczywisty charakter regulatora Aktualna propozycja nazwy organu regulacyjnego brzmi wprawdzie znakomicie, jednak nie oddaje tego czym w rzeczywistości ma się zajmować. Jedynym zadaniem związanym z rozwojem opisanym w ustawie są piaskownice legislacyjne, co samo w sobie nie jest rozwojem sztucznej inteligencji, ani rozwojem systemów sztucznej inteligencji, a jedynie przygotowaniem narzędzia pozwalającego na sprawdzanie zgodności rozwiązania z wymaganiami. Co więcej, nie jest to elementem polskiej strategii rozwoju sztucznej inteligencji, a obowiązkiem wynikającym z AI Act. Jedynym zadaniem związanym z bezpieczeństwem opisanym w ustawie jest zbieranie informacji o poważnych incydentach. Ponownie, mówimy o obowiązku wynikającym z europejskiej regulacji. Widać zatem, że zarówno tworzenie warunków rozwoju sztucznej inteligencji (modeli, systemów), jak i kwestie bezpieczeństwa w zdecydowanej części i za wyjątkiem dwóch wymienionych wyżej działań leżą w kompetencji innych organów państwa. Wreszcie sama ustawa mówi o systemach sztucznej inteligencji, zaś nazwa Komisji nie zawiera słowa„systemy”. Podobnie jak w przypadku innych organów regulacyjnych istotne jest, aby nazwa Komisji oddawała jej prawdziwy charakter i rodzaj wykonywanych zadań.
AmCham	art. 6 ust. 2	W świetle projektowanych przepisów Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji ma się składać wyłącznie z przedstawicieli następujących organów: Prezes UOKiK, KNF, Rzecznik Praw Dziecka,

		KRRiT, Prezesa UKE, Państwowej Inspekcji Pracy oraz Prezesa Urzędu Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych. Zatem Komisja ma się składać wyłącznie z przedstawicieli organów regulacyjnych, których głównym zadaniem jest kontrola, nadzór i egzekwowanie przestrzegania sektorowych przepisów prawa, w tym nakładanie kar pieniężnych. Trudno wyobrazić sobie, aby Komisja, składająca się wyłącznie z przedstawicieli organów kontroli i nadzoru, faktycznie była w stanie perspektywę inną niż ta wynikająca z doświadczeń w zakresie kontroli i nadzoru. Celem zapewnienia zrównoważonego i odpowiedzialnego rozwoju sztucznej inteligencji w Polsce, Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji powinna zostać poszerzona o przedstawicieli środowisk naukowych, pracodawców i przedsiębiorców, ze względu na swoją nadrzędną rolę w kształtowaniu polityki AI. Obecność ekspertów z tych dziedzin wzbogaciłaby Komisję o niezbędną wiedzę specjalistyczną i zapewniłaby zrównoważone podejście do rozwoju sztucznej inteligencji w Polsce. Włączenie przedstawicieli nauki, takich jak profesorowie uniwersytetów, badacze z instytutów naukowych czy eksperci z organizacji pozarządowych, pozwoliłoby Komisji uwzględniać najnowsze osiągnięcia badawcze i trendy technologiczne w dziedzinie AI. To z kolei umożliwiłoby podejmowanie decyzji opartych na rzetelnej wiedzy naukowej. Dzięki temu Polska mogłaby skuteczniej konkurować na arenie międzynarodowej w dziedzinie badań i rozwoju AI, przyciągając inwestycje i talenty z zagranicy. Z kolei obecność przedstawicieli organizacji przedsiębiorców w Komisji zapewniłaby lepsze zrozumienie praktycznych aspektów wdrażania AI w biznesie. Ich doświadczenie i wiedza byłyby nieocenione przy tworzeniu regulacji, które sprzyjałyby innowacjom i inwestycjom. Podsumowując, poszerzenie składu Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji o przedstawicieli środowisk naukowych, pracodawców i przedsiębiorców jest niezbędne, aby zapewnić zrównoważony i odpowiedzialny rozwój sztucznej inteligencji w Polsce. Tylko takie kompleksowe podejście, uwzględniające perspektywy różnych dziedzin i sektorów, pozwoli na wykorzystanie potencjału AI dla dobra

		całego społeczeństwa, jednocześnie minimalizując ryzyko związane z jej zastosowaniem. W ten sposób Polska może stać się liderem w dziedzinie sztucznej inteligencji, kształtując przyszłość technologii w sposób odpowiedzialny i zrównoważony.
AmCham	art. 6 ust. 2a w związku z art. 6 ust. 3 oraz art. 5 ust. 3	Propozycja: wprowadzenie art. 6 ust. 2a w brzmieniu „Przewodniczący Komisji zaprasza z głosem doradczym podmioty wymienione w art. 5 ust. 3 do udziału w posiedzeniu Komisji.” Uzasadnienie: Art. 6 ust. 3 daje swobodę zapraszania różnych podmiotów na posiedzenia Komisji („może zaprosić do udziału”). Tymczasem w przypadku podmiotów, które są wymienione w art. 5 ust. 3 wykonanie tej kompetencji powinno mieć charakter obligatoryjny. Oczywiście głos tych podmiotów jest wyłącznie głosem doradczym. Bez takiego zapisu „współpraca”, o której mowa w art. 5 ust. 3 staje się dość nieczytelna. Proponowany zapis jest szczególnie istotny w świetle zmian składu Komisji, jaki został zaprezentowany w wersji projektu ustawy z lutego 2025. Nieobecność reprezentantów Rzecznika Praw Obywatelskich i Prezesa Urzędu Ochrony Danych Osobowych jest szczególnie rzucająca się w oczy. Natomiast, bez uszczerbku dla ustawowych kompetencji tych organów, ich obligatoryjne zapraszanie na posiedzenia Komisji miałoby walor dochowania należytej staranności przy wypracowywanych przez Komisję stanowiskach, decyzjach czy rekomendacjach.
AmCham	art. 9 ust. 5, art. 10 ust. 1 i 2, art. 12 ust. 1 i 2, art. 13	Przepisy dają polskim władzom dużą swobodę w zakresie publikowania interpretacji Aktu o AI. Rodzi to poważne ryzyko fragmentacji prawa UE. Zakładając, że poszczególne organy ds. sztucznej inteligencji państw członkowskich będą miały podobne uprawnienia, będzie to prowadzić do różnych interpretacji Aktu, a w konsekwencji do rozbieżności w wykładni i stosowaniu. Doprowadzi to do stanu niepewności regulacyjnej, co negatywnie wpłynie na rozwój sztucznej inteligencji w całej UE. Sugerujemy, aby w przepisach krajowych wyraźnie wspomniano, że wszystkie wytyczne krajowe powinny być zgodne z Aktem o AI i wytycznymi Biura ds. AI.
AmCham	art. 12 ust. 3 pkt 2	Proponujemy, aby własne stanowisko podmiotu składającego wniosek o opinię indywidualną było opcjonalne, a nie wymagane.

AmCham	art. 22 ust. 5	Celem zapewnienia solidnych ram ochrony danych w kontekście sztucznej inteligencji, konieczne jest wprowadzenie bardziej rygorystycznych środków bezpieczeństwa, które będą regulować ujawnianie informacji poufnych podmiotom zewnętrznym, w tym organom ścigania. Jednym z podstawowych zabezpieczeń może być wprowadzenie obowiązku uzyskania uprzedniej zgody sądu lub prokuratora przed udostępnieniem takich danych. To dodatkowe wymaganie zapewniłoby, że ujawnienie danych nastąpi tylko wtedy, gdy istnieje wyraźna, uzasadniona podstawa prawna i nie narusza to innych istotnych praw. Alternatywnie lub dodatkowo, można dostosować obecne ramy prawne do standardów poufności zawartych w Prawie o komunikacji elektronicznej. Takie dostosowanie zapewniłoby spójne i kompleksowe podejście do ochrony wrażliwych informacji w różnych sektorach, w tym w obszarze AI. Należy podkreślić, że dane związane z AI często obejmują nie tylko cenne informacje biznesowe i rynkowe, ale także krytyczne szczegóły operacyjne firm zaangażowanych w rozwój i wdrażanie AI. Nieuprawnione ujawnienie takich danych może mieć poważne konsekwencje, takie jak utrata przewagi konkurencyjnej, szkody finansowe, a nawet zagrożenie dla bezpieczeństwa narodowego. W związku z tym niezbędne jest ustanowienie mechanizmów prawnych, które skutecznie zapobiegną nieuzasadnionemu udostępnianiu danych związanych z AI. Obecnie istnieje ryzyko, że takie dane mogą być udostępniane bez odpowiedniej kontroli, co może prowadzić do niezamierzonego ujawnienia tajemnic przedsiębiorstwa, zastrzeżonych algorytmów lub strategicznych decyzji biznesowych. Wdrożenie kontroli sądowej lub prokuratorskiej stanowiłoby istotne zabezpieczenie przed potencjalnymi nadużyciami i zapewniłoby, że dostęp do wrażliwych danych AI jest przyznawany tylko wtedy, gdy istnieje wyraźna i uzasadniona potrzeba, np. w ramach prowadzonego postępowania karnego. Taki mechanizm zwiększyłby również zaufanie do ram regulacyjnych i zapewniłoby ochronę praw wszystkich zainteresowanych stron.
AmCham	art. 23 ust. 4	Proponujemy wykreślenie tego ustępu, ponieważ przepisy RODO bardzo wyraźnie określają ograniczenie przetwarzania w art. 5 ust. 1 punkt e,

		mówiąc, że „Dane osobowe muszą być: (…) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”)”, a zatem nie powinno się z góry zakładać dwuletniego okresu przechowywania, który może przerwać dopiero przegląd danych, a ograniczyć przechowywanie w zgodzie z przepisami RODO.
AmCham	art. 27 ust. 2	Obecna redakcja przepisu może sugerować, że opinie lub stanowiska Rady wyrażane w innym trybie niż opisanym w art. 27 ust. 1 punkt 1) są dla Komisji wiążące, co nie wydaje się zgodne z intencją projektodawcy.
AmCham	art. 36 ust. 1	Nastąpiło zmniejszenie liczby ministrów właściwych dla swoich działów administracji, którzy mogą w drodze porozumienia powierzyć Komisji realizację zadań. Ograniczenie to nie wydaje się celowe
AmCham	art. 39 ust. 3	Wprowadzenie obowiązku zdalnych inspekcji centrów danych i usług w chmurze budzi poważne obawy dotyczące bezpieczeństwa danych i prywatności. Wymagania cyberbezpieczeństwa wobec inspektorów, ich urządzeń, systemów i aplikacji mogą być istotnie niższe niż wobec personelu obsługującego centra danych. Tym samym mogą narażać wrażliwe dane zwiększając ryzyko incydentów lub naruszeń. Firmy będą potrzebować solidnych zapewnień, że procesy inspekcji są bezpieczne, zwłaszcza podczas bieżącej obsługi klientów. Potencjalny dostęp do logów lub rejestrów zawierających dane osobowe lub poufne dane biznesowe, w tym tajemnice przedsiębiorstwa, wprowadza dodatkowe wyzwania związane z prywatnością i zgodnością. Zdalne inspekcje mogą również prowadzić do ryzyk związanych z cyberbezpieczeństwem. Udzielanie zewnętrznego dostępu może wprowadzić nowe podatności. Zakłócenia operacyjne to kolejna obawa, ponieważ zdalne inspekcje systemów pracujących w czasie rzeczywistym mogą zakłócać regularne

		operacje, wpływając na wydajność systemu lub świadczenie usług klientom. Dla firm posiadających systemy krytyczne dla usług w czasie rzeczywistym, czas i metoda inspekcji będą wymagały starannej koordynacji w celu zminimalizowania przerw w świadczeniu usług. Zgodność z wymaganiami dotyczącymi lokalizacji danych może stać się problemem w niektórych jurysdykcjach. Zdalne inspekcje mogą kolidować z tymi przepisami, jeśli inspektorzy są zlokalizowani poza krajem, co może narażać firmy na ryzyko prawne. To ostatnie dotyczy nie tylko dostawców usług, ale także podmioty wykorzystujące systemy sztucznej inteligencji. Zakres i kontrola dostępu do inspekcji będą musiały być starannie zdefiniowane. Udzielanie zbyt szerokiego dostępu może prowadzić do niezamierzonego ujawnienia niepowiązanych wrażliwych danych, co sprawia, że konieczne jest wdrożenie ścisłych mechanizmów kontroli dostępu i audytu w celu monitorowania działań inspektorów, co może być technicznie skomplikowane i wymagać dużych zasobów. Wiele firm ma zobowiązania umowne do ochrony danych klientów, a zdalne inspekcje mogą naruszać te umowy, ryzykując utratę reputacji i zaufania. Rozwianie tych obaw wymagałoby kompleksowego podejścia, w tym rygorystycznych środków bezpieczeństwa, precyzyjnych ograniczeń dostępu, zgodności z prawem oraz jasnej odpowiedzialności za wszelkie naruszenia danych lub niewłaściwe postępowanie. Podsumowując: zapisy art. 42 ust. 3 są dalece niewystarczające dla zapewnienia bezpiecznej kontroli, nienaruszającej działalności operacyjnej.
AmCham	art. 40 ust. 2, art. 40 ust. 4 w kontekście art. 40 ust. 9	Przepis wskazujący, że dopuszczona do kontroli osoba trzecia musi wykazywać się wyłącznie wiedzą specjalistyczną jest dalece niewystarczający. Podmioty kontrolowane, a także ich klienci, wymagają znacznie większej ochrony poufności i tajemnic przedsiębiorstw niż jest to zapisane w propozycji.
AmCham	art. 42	Analizując język Artykułu 42, wydaje się on być na tyle szeroki, że wyznaczeni inspektorzy mogliby żądać dostępu do treści klientów przechowywanych w kontach chmurowych. Taki zakres kontroli wydaje się być niezgodny z Artykułem 78(2) Aktu o AI,

		który zezwala organom na żądanie wyłącznie danych ściśle niezbędnych do realizacji zadań związanych z oceną zgodności i egzekwowaniem Aktu o AI, podczas gdy Artykuł 42 ust. 1 wyraźnie wspomina o dostępie do systemów informatycznych i chmury obliczeniowej należącej do innego podmiotu, zawierających dane Kontrolowane związane z przedmiotem kontroli, w zakresie, w jakim kontrolowany ma do nich dostęp. Zdanie odnoszące się do "systemu informatycznego i chmury obliczeniowej należącej do innej strony" powinno zostać usunięte. Argumentacja: Żaden przepis tej ustawy nie może być interpretowany jako wymagający ujawnienia danych klientów przechowywanych przez dostawcę usług chmurowych. W takich przypadkach inspektor powinien przekierować żądanie do administratora danych (klienta) w celu uzyskania żądanych informacji. Jest to zgodne z ustalonymi wytycznymi organów ścigania w wielu krajach dotyczącymi pozyskiwania danych należących do klientów korporacyjnych i biznesowych, przechowywanych u dostawcy usług chmurowych. Należy zauważyć, że dostawcy usług chmurowych nie mają wglądu w treści przechowywane w imieniu klientów, co uniemożliwia określenie, jakie "pisma, dokumenty lub inne informacje" mogą być przechowywane przez klienta i czy są one istotne dla audytu inspektora. Ponadto, klienci korporacyjni i biznesowi zazwyczaj przechowują dane należące do ich własnych użytkowników końcowych i klientów, więc przymusowe udostępnienie takich danych może skutkować niewłaściwym ujawnieniem danych należących do podmiotów, które nie są przedmiotem lub nie są istotne dla danego audytu
AmCham	art. 46 ust. 4	W celu zapewnienia rzetelności i efektywności procesu kontrolnego, a także zagwarantowania prawa do obrony, termin na wniesienie zastrzeżeń do raportu z kontroli powinien wynosić co najmniej 14 dni. Obecnie zapisany w projekcie ustawy termin 7 dni w wielu przypadkach będzie niewystarczający, w szczególności w przypadku obszernych i szczegółowych raportów, zawierających analizę dużej ilości danych,

		materiałów, informacji i dokumentów. Analiza i przygotowanie uwag i zastrzeżeń będzie wymagało więcej czasu niż 7 dni. Zapewnienie 14 dni na zgłoszenie uwag do raportu z kontroli umożliwi kontrolowanym podmiotom dokładne zapoznanie się z treścią raportu, przeprowadzenie własnych analiz i konsultacji, a w konsekwencji – przygotowanie rzeczowych i wyczerpujących zastrzeżeń. Zapewni to również większą transparentność i obiektywizm procesu kontrolnego, co przyczyni się do zwiększenia zaufania do jego wyników.
AmCham	art. 53	Projekt ustawy w wersji z lutego 2025 roku wprowadza istotne zmiany w zakresie uprawnień Komisji, poszerzając jej kompetencje w obszarze wydawania ostrzeżeń. Zgodnie z nowymi przepisami, ostrzeżenia Komisji nabierają charakteru władczego, a ich zignorowanie może skutkować poważnymi konsekwencjami dla dostawców AI. Wśród potencjalnych sankcji, które może zastosować Komisja, jeśli adresat nie zastosuje się do “ostrzeżenia” Komisji, projekt ustawy wymienia m.in. nakaz zablokowania systemu, uniemożliwienie dostępu użytkownikom końcowym, a nawet nałożenie kary pieniężnej. Takie rozwiązanie budzi jednak poważne wątpliwości, gdyż stoi w sprzeczności z samą naturą ostrzeżenia, które powinno być instrumentem o charakterze "miękkim", niewładczym. W świetle projektowanych przepisów, wydanie “ostrzeżenia” nie wymaga od Komisji udowodnienia naruszenia, wystarczyć ma jedynie uzasadnione podejrzenie. Ponadto, zgodnie z projektowanymi przepisami ostrzeżenie ma formę postanowienia (a nie decyzji administracyjnej). W efekcie projektowane przepisy, dają Komisji możliwość nakładania kar pieniężnych bez konieczności udowodnienia naruszenia i bez wydawania decyzji administracyjnej, tworząc sytuację, w której na podstawie jedynie uzasadnionego podejrzenia, bez przeprowadzenia pełnego postępowania administracyjnego dostęp do systemu AI może zostać zablokowany a dostawcy AI mogą być pociągnięci do odpowiedzialności finansowej. Biorąc powyższe pod uwagę projektowane przepisy należy zmienić tak, aby ostrzeżenie - zgodnie ze swoją nazwą i naturą - faktycznie było "miękki", nie władczym narzędziem w rękach Komisji. W przypadku niezastosowania się do ostrzeżenia, Komisja powinna mieć możliwość

		skorzystania z innych narzędzi przewidzianych w projektowanej ustawie, takich jak kontrole czy wydawanie decyzji administracyjnych po przeprowadzeniu odpowiedniego postępowania kontrolnego. Takie rozwiązanie pozwoliłoby na zachowanie równowagi między koniecznością zapewnienia bezpieczeństwa użytkowników a ochroną praw dostawców AI.
AmCham	art. 53 ust. 3	Zapisany w projekcie ustawy 14-dniowy termin na zastosowanie się do ostrzeżeń Komisji i wdrożenie środków naprawczych w celu usunięcia skutków naruszenia jest niewystarczający. Wdrożenie zmian wynikających z ostrzeżenia Komisji może być czasochłonne, wymagając np. i) zmian w kodzie, które muszą zostać dokładnie przetestowane przed wdrożeniem na środowisku produkcyjnym, aby zapewnić ich poprawność i niezawodność, ii) przeprowadzenia oceny bezpieczeństwa, których celem będzie zweryfikowanie, czy wprowadzane zmiany nie generują zagrożeń dla bezpieczeństwa systemu, a filanie iii) przeprowadzenia kontroli zgodności z przepisami, mające na celu zapewnienie, że wszelkie modyfikacje są zgodne z wieloma, często nakładającymi się na siebie ramami prawnymi, co jest szczególnie istotne w przypadku organizacji działających na wielu rynkach. Biorąc pod uwagę te czynniki, widzimy potrzebę zmiany projektowanych przepisów tak, aby to Komisja, wydając ostrzeżenie, określała termin w jakim oczekuje wykonania zaleceń wskazanych w ostrzeżeniu, przy czym projektowana ustawa powinna wskazywać, że termin wyznaczony przez Komisję nie może być krótszy niż 30 dni od dnia otrzymania ostrzeżenia przez adresata. Takie rozwiązanie zapewni, że adresaci ostrzeżeń zawsze będą mieli co najmniej 30 dnia na wprowadzenie zmian i dostosowanie się do ostrzeżenia, a jednocześnie zapewni Komisji niezbędną elastyczność i możliwość wyznaczenia dłuższego terminu, gdyż w praktyce mogą wystąpić sytuacje, w których sama Komisja może uznać, że szczególne okoliczności sprawy wymagają, aby adresat ostrzeżenia miał więcej niż 30 dni na dostosowanie się.
AmCham	art. 55 ust. 2	Art. 55 ust. 2 w obecnym kształcie jest najbardziej kontrowersyjnym przepisem projektowanej ustawy, który może wyrządzić najwięcej szkody. Z tego względu prosimy o priorytetowe potraktowanie naszych uwag w tym

		zakresie. Przepis przyznający Komisji uprawnienie do nakazania operatorowi systemu zaprzestania korzystania z systemu lub wycofania go z rynku lub użytku publicznego jest zbyt szeroki i niejasny, gdyż nie sposób uznać, że jasną i jednoznaczną przesłanką jest " [...] wywiera lub poprzez swoje działanie może wywrzeć wpływ na opinie i nastroje społeczne w stopniu istotnym dla wyniku mających się odbyć w terminie nie dłuższym niż 30 dni od stwierdzenia tego ryzyka w odniesieniu do wyborów [...]". Na gruncie tak sformułowanego przepisu Komisja będzie miała w zasadzie dowolność oceny, czy zasadne jest zastosowanie tego przepisu. Brak konkretnych i obiektywnych kryteriów, które Komisja miałaby stosować przy podejmowaniu takiego rozstrzygnięcia, stwarza ryzyko arbitralności i nadużyć. A skutki zastosowania tego przepisu przez Komisję będą dalekosiężne, wręcz drastyczne dla dostawców modeli sztucznej inteligencji, gdyż w takim przypadku Komisja ma mieć możliwość nakazania operatorowi systemu sztucznej inteligencji zaprzestanie stosowania lub wycofanie systemu z rynku lub użytku, czyli de facto nakaz zamknięcia usługi. Na domiar złego Komisja może nakazać natychmiastowe wykonanie nakazu, wyłączając możliwość weryfikacji rozstrzygnięcia Komisji jeszcze przed koniecznością zamknięcia systemu. Natychmiastowa wykonalność tak kontrowersyjnego rozstrzygnięcia podważa prawo do kontroli sądowej, ponieważ strona, której dotyczy decyzja, miałaby ograniczoną możliwość zakwestionowania jej przed poniesieniem potencjalnie nieodwracalnych konsekwencji. W praktyce oznacza to, że decyzja Komisji mogłaby być wykonana zanim sąd zdążyłby ją zbadać i ewentualnie wstrzymać jej wykonanie. W efekcie projektowany przepis daje Komisji możliwość wydawania rozstrzygnięć o daleko idących skutkach (włącznie z wyłączeniem możliwości korzystania z systemu AI), egzekwowanych w trybie natychmiastowym, bez realnej możliwości skutecznego odwołania się do sądu, a wszystko w oparciu o bardzo nieprecyzyjne i ocenne kryteria. W skrajnie negatywnym scenariuszu analizowane uprawnienie Komisji mogłoby być wykorzystywane politycznie, co jest szczególnie niebezpieczne w kontekście wyborów, a więc w kontekście, do którego wprost odnosi się analizowany przepis. Nie sposób nie zauważyć, że tego typu regulacji nie ma (i nie powinno być)

		w obszarze np. mediów, a przecież to media, a nie sztuczna inteligencja, mają większe znaczenie w przypadku wyborów. Tworząc regulacje prawne dotyczące sztucznej inteligencji należy zachować zdrowy rozsądek i nie demonizować tej technologii. Ponadto, analizowane narzędzie nie ma podstaw i nie ma odpowiednika w Akcie o AI i stanowi ewidentny przykład gold-platingu, którego w polskiej regulacji miało nie być. Co więcej, jest to gold-plating bardzo kontrowersyjny i szkodliwy z perspektywy tworzenia bezpiecznego otoczenia prawnego dla rozwoju sztucznej inteligencji w Polsce. Ponadto, już sam fakt, że mówimy o gold-platingu rodzi pytania o zgodność projektowanego rozwiązania z prawem UE, skoro Akt o AI jest rozporządzeniem (a nie dyrektywą), co formalnie oznacza, że nie wymaga implementacji, a w prawie krajowym nie powinno być przepisów dotyczących AI, które wykraczają poza czy ponad przepisy Aktu o AI. W związku z powyższym, analizowany przepis powinien zostać całkowicie usunięty z projektu ustawy, a uprawnienia Komisji powinny być ściśle ograniczone do zakresu określonego w art. 79 Aktu o AI, aby zapewnić zgodność z prawem UE i uniknąć niepotrzebnych i szkodliwych ograniczeń w rozwoju sztucznej inteligencji w Polsce.
AmCham	art. 71	Stoimy na stanowisku, że kary powinny być ograniczone do spółek dopuszczających się naruszenia.
AmCham	art. 78 ust. 1	24-godzinny termin na zgłoszenie poważnych incydentów będzie stanowił wyzwanie dla efektywnego zarządzania i reagowania na incydenty, szczególnie w kontekście złożonych struktur organizacyjnych i zaawansowanych systemów, takich jak sztuczna inteligencja. W przypadku poważnych incydentów priorytetem jest i powinno być natychmiastowe podjęcie działań naprawczych i mitygujących skutki incydentu, a nie raportowanie incydentu do organów administracji. Wyznaczenie bardzo krótkiego terminu na zgłoszenie incydentu w sposób oczywisty wymusi przydzielanie zasobów do przygotowania zgłoszenia w momencie, w którym wszystkie dostępne zasoby powinny być zaangażowane w działania naprawcze i mitygujące. Przygotowanie i przekazanie zgłoszenia poważnego incydentu w większości przypadków wymagać będzie:

		• analizy incydentu: identyfikacji przyczyn, oceny skutków oraz potencjalnego wpływu; • zebrania niezbędnych danych: zgromadzenie dowodów, logów oraz innych informacji istotnych dla zrozumienia incydentu; • koordynacji działań wewnątrz organizacji; • przygotowanie raportu zawierającego wszystkie istotne informacje dotyczące incydentu. I w większości przypadków wykonanie wszystkich wyżej wymienionych kroków nie będzie możliwie w 24 godziny. Co więcej, art. 73 Aktu o AI stanowi: „Zgłoszenia, o którym mowa w ust. 1, dokonuje się niezwłocznie po ustaleniu przez dostawcę związku przyczynowego między systemem AI a poważnym incydentem lub uzasadnionego prawdopodobieństwa wystąpienia takiego związku, a w każdym razie nie później niż w terminie 15 dni od dnia, w którym dostawca lub, w stosownych przypadkach, podmiot wdrażający dowiedział się o poważnym incydencie". Nie widać istotnego powodu by ten termin radykalnie skracać. Projekt ustawy powinien przewidywać przynajmniej 7 dni na zgłoszenie poważnego incydentu. Zapewnienie racjonalnego terminu raportowania poważnych incydentów przyczyni się do większej jakości raportowania, umożliwi skuteczne reagowanie na incydenty oraz umożliwi organizacjom lepsze zarządzanie ryzykiem.
AmCham	art. 78 ust. 2 pkt 4, lit. b	Proponujemy zastąpić w tym przepisie słowo „użytkowników" słowem „osób". Wynika to z definicji incydentu poważnego.
AmCham	art. 78 ust. 2, pkt 4, lit g.	Jest: ocenę „dotkliwości poważnego incydentu, w szczególności w odniesieniu do zdrowia, bezpieczeństwa i praw podstawowych osób" Propozycja: „wpływ na zdrowie, bezpieczeństwo i prawa podstawowe osób" „Dotkliwość" incydentu nie jest nigdzie zdefiniowana. Proponowane sformułowanie przepisu jest bardziej precyzyjne.
AmCham	art. 85 ust. 1	Wymieniony został wyłącznie art. 57 ust. 9 rozporządzenia 2024/1689. Uważamy, że należy wskazać także ust. 5 tego samego artykułu.

AmCham	art. 94 ust. 2	Jest: Minister właściwy do spraw informatyzacji do 31 marca każdego roku przekazuje Radzie Ministrów oraz Komisji informację na temat wymaganych zasobów obliczeniowych do dalszego rozwoju systemów sztucznej inteligencji i prognozowanego zużycia energii z tego tytułu. Propozycja: Minister właściwy do spraw informatyzacji, w porozumieniu z ministrem właściwym do spraw nauki i szkolnictwa wyższego, do 31 marca każdego roku przekazuje Radzie Ministrów oraz Komisji informację na temat zasobów obliczeniowych w sektorze finansów publicznych oraz sektorze nauki i szkolnictwa wyższego wymaganych do dalszego rozwoju systemów sztucznej inteligencji i prognozowanego zużycia energii z tego tytułu. Nie istnieją w chwili obecnej żadne standardy dotyczące raportowania dla całego przemysłu teleinformatycznego. Co więcej, zasoby w Polsce mogą być także wykorzystywane przez podmioty z innych krajów co dodatkowo tylko będzie zaciemniało obraz. Natomiast informacja o niezbędnych zasobach w sektorze publicznym oraz w polskiej nauce będzie istotną informacją dla planowanego rozwoju tej dziedziny w naszym kraju.
AmCham	rozdział 9 (art. 97-106)	Stoimy na stanowisku, że umieszczenie w projekcie ustawy przepisów karnych jest niecelowe. Sankcje karne miałyby znaczący efekt odstraszający i poważnie ograniczyłyby rozwój i wdrażanie sztucznej inteligencji w Polsce. Zdecydowanie bardziej sensowne i bardziej spójne z aktem o AI byłoby konsekwentne stosowanie administracyjnych kar pieniężnych.
AmCham	art. 99	Projektowany przepis zezwala na finansowanie Urzędu Komisji z wpływów pochodzących z kar pieniężnych nakładanych przez Komisję. Z oczywistych wręcz względów jest to rozwiązanie wysoce kontrowersyjne. Przepis w tym kształcie prowadzi do sytuacji, w której Komisja będzie silnie zmotywowana do nakładania wysokich i licznych kar pieniężnych, nie ze względu na rzeczywiste naruszenia przepisów prawa, ale w celu poprawy swojej sytuacji finansowej. Takie rozwiązanie jest nieetyczne i szkodliwe dla rozwoju sztucznej inteligencji w Polsce. System, w którym organ ma bezpośrednią korzyść finansową z nakładania kar, zachęca go do nadużywania swoich uprawnień. Zamiast wspierać

		innowacje i rozwój technologii, Komisja może skupić się na poszukiwaniu błahych uchybień, które pozwolą jej na generowanie dodatkowych przychodów. Taka praktyka z pewnością zniechęci przedsiębiorców i inwestorów do angażowania się w projekty związane ze sztuczną inteligencją w Polsce. Co więcej, przepis ten stoi w sprzeczności z innymi rozwiązaniami proponowanymi w projekcie ustawy, które mają na celu wspieranie rozwoju sztucznej inteligencji, takimi jak piaskownice regulacyjne. Piaskownice regulacyjne służą temu, aby firmy mogły testować innowacyjne rozwiązania w kontrolowanym środowisku, bez obawy o surowe kary finansowe. Jeśli jednak Komisja będzie miała motywację do nakładania wysokich kar, idea piaskownic regulacyjnych zostanie wypaczona. Rozwiązanie, w którym kary pieniężne stanowią przychód organu nakładającego kary, jest niezgodne z europejskimi i polskimi standardami. W Polsce, organy takie jak Prezes Urzędu Ochrony Konkurencji i Konsumentów, Prezes Urzędu Komunikacji Elektronicznej czy Prezes Urzędu Ochrony Danych Osobowych nie czerpią korzyści finansowych z nakładanych kar. Wpływy z kar nakładanych przez te organy trafiają albo do budżetu państwa albo do specjalnych funduszy celowych, które mają osobowość prawną i są niezależne od organów nakładających kary. Zasada ta powinna być również stosowana w przypadku Komisji. Wpływy z kar pieniężnych nakładanych przez Komisję powinny trafiać do budżetu państwa, a nie do budżetu Komisji. Tylko takie rozwiązanie zapewni bezstronność i obiektywizm Komisji oraz przyczyni się do zdrowego rozwoju sztucznej inteligencji w Polsce.