

Warszawa, 4 września 2025 r.
KL/407/139/ET/2025

Pan

Mariusz Skowroński

Sekretarz Stałego Komitetu Rady Ministrów

Kancelaria Prezesa Rady Ministrów

Pan

Dariusz Standerski

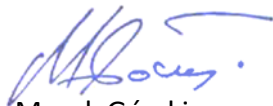
Sekretarz Stanu

Ministerstwo Cyfryzacji

Szanowni Państwo,

w związku ze skierowaniem Projektu ustawy o systemach sztucznej inteligencji (UC71) pod obrady Stałego Komitetu przedstawiamy w załączeniu stanowisko Konfederacji Lewiatan.

Z poważaniem



Marek Górski

Prezydent Konfederacji Lewiatan

Załącznik: Stanowisko Konfederacji Lewiatan do Projektu ustawy o systemach sztucznej inteligencji (UC71)

Do wiadomości:

- Pan Maciej Berek – Minister nadzoru nad wdrażaniem polityki rządu, szef SKRM
- Pani Pamela Krzyrkowska – Dyrektorka, Departament Badań i Innowacji, Ministerstwo Cyfryzacji

member of



BUSINESSatOECD

member of



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

Stanowisko Konfederacji Lewiatan do Projektu ustawy o systemach sztucznej inteligencji (UC71)

Szczególnie pozytywnie oceniamy najnowsze zmiany dotyczące opinii indywidualnych, mówiące o tym, że zastosowanie się do opinii indywidualnej przed jej zmianą, stwierdzeniem nieważności albo uchynieniem nie może szkodzić podmiotowi, któremu opinia indywidualna została wydana. Dzięki temu możliwe jest poleganie na opiniach, bez obaw o negatywne skutki. Jest to szczególnie istotne dla przedsiębiorców, którym zależy na stabilności otoczenia regulacyjnego i pewności co do skutków podejmowanych działań. Doceniamy również możliwość zasięgania przez Komisję opinii innych organów państwowych oraz wyspecjalizowanych jednostek organizacyjnych w toku przygotowywania opinii indywidualnych. Takie rozwiązanie powinno przełożyć się na wyższą jakość merytoryczną i większą trafność wydawanych interpretacji. Pozytywnie oceniamy także wprowadzenie obowiązku publikacji aktualnych opinii indywidualnych – po uprzednim usunięciu danych identyfikujących oraz informacji stanowiących tajemnice prawnie chronione – w Biuletynie Informacji Publicznej. Uzupełnienie tego obowiązku o komunikaty dotyczące zmian w przepisach prawa, orzecznictwie oraz wytycznych, które mogą wpływać na ważność wydanych opinii, odbieramy jako istotne narzędzie wspierające prawidłową wykładnię przepisów oraz zwiększającym pewność prawa.

1. Art. 2 oraz art. 2 ust. 2

Uwagi:

Art. 2 ust. 2, odnoszący się do modeli AI ogólnego przeznaczenia (GPAI), jest niejasny i może prowadzić do nadregulacji na poziomie krajowym, co stoi w sprzeczności z kompetencjami unijnego Biura ds. AI. Niejasne przepisy dotyczące modeli GPAI mogą doprowadzić do sytuacji, w której polski organ wejdzie w spór kompetencyjny z unijnym Biurem ds. AI, co podważy pozycję Polski jako przewidywalnego środowiska regulacyjnego. Dlatego precyzyjne określenie zakresu w samej ustawie poprzez odesłanie do AI Aktu w zakresie w jakim odnosi się do modeli GPAI nie jest nadmiarowe, lecz stanowi fundament pewności obrotu gospodarczego i zapobiega przyszłym, kosztownym sporom prawnym.

Proponowane brzmienie:

~~2. O ile przepisy ustawy nie stanowią inaczej, przepisy w zakresie systemów sztucznej inteligencji mają zastosowanie również do modeli sztucznej inteligencji ogólnego~~

member of



member of



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

~~przeznaczenia.~~ Przepisy ustawy stosuje się do modeli sztucznej inteligencji ogólnego przeznaczenia w zakresie wynikającym z Rozporządzenia 2024/1689.

2. Art. 36 ust. 1

Uwagi:

Uprawnienie kontrolujących do żądania dostępu do „chmury obliczeniowej będącej własnością innego podmiotu” (art. 36 ust. 1 pkt 1 projektu) jest sformułowane zbyt szeroko. Stwarza to istotne ryzyko naruszenia tajemnicy przedsiębiorstwa oraz praw podstawowych (w tym prawa do prywatności) klientów podmiotu kontrolowanego, którzy nie są stroną postępowania.

Pochwalamy potrzebę zapewnienia kontrolującym skutecznych narzędzi do weryfikacji, która nie zawsze jest możliwa na podstawie dokumentacji. Jednak obecne postanowienie, pozwalające na dostęp do chmury podmiotu trzeciego, narusza zasadę proporcjonalności i stwarza ogromne ryzyko prawne dla samego organu nadzoru. Organ może wejść w posiadanie danych nieobjętych kontrolą, w tym tajemnic handlowych i danych osobowych klientów kontrolowanego, co będzie stanowić podstawę do postępowań odszkodowawczych przeciwko Skarbowi Państwa.

Uzyskanie przez kontrolującego danych niezwiązanych z kontrolą, w tym danych osobowych klientów mogłoby zostać zakwestionowane jako działanie wykraczające poza dopuszczalny zakres kontroli wskazany w art. 78 ust. 2 samego AI Aktu.

Proponowane rozwiązanie:

Proponujemy zatem doprecyzowanie przepisu poprzez dodanie odniesienia do RODO oraz art. 78 ust. 2 AI Aktu, który wyraźnie ogranicza zakres danych możliwych do pozyskania przez organy kontrolne do tych, które są bezwzględnie konieczne do oceny ryzyka związanego z systemami AI i wykonywania uprawnień nadzorczych.

3. Art. 40 oraz art. 47

Uwagi:

Terminy przewidziane w projekcie na realizację obowiązków proceduralnych, takie jak 7 dni na zgłoszenie zastrzeżeń do protokołu kontroli (art. 40 ust. 4) czy 14 dni na wykonanie ostrzeżenia Przewodniczącego Komisji (art. 47 ust. 3), są zbyt krótkie. W przypadku złożonych systemów AI, przygotowanie merytorycznej odpowiedzi w tak krótkim czasie jest często niemożliwe.

member of



member of



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

Zapewnienie odpowiednio szybkiej ochrony użytkowników jest konieczne, niemniej w praktyce tak krótkie terminy przyniosą skutek odwrotny. Uniemożliwią przedsiębiorcy rzetelne zbadanie problemu technicznego i przygotowanie merytorycznej odpowiedzi oraz skutecznego planu naprawczego. W efekcie organ otrzyma odpowiedzi powierzchowne, a ewentualne spory będą musiały być przenoszone do sądów, co znacząco wydłuży, a nie skróci, czas ostatecznego rozwiązania problemu.

Proponowane rozwiązanie:

Wydłużenie terminów do **co najmniej 60 dni** nie osłabi ochrony użytkowników, lecz ją wzmocni, ponieważ pozwoli na dogłębną analizę i wdrożenie skutecznych, a nie pozornych, działań naprawczych już na etapie przedsądowym. Jest to w interesie zarówno przedsiębiorców, jak i samego organu nadzoru, który zyska na jakości współpracy.

4. Art. 47 oraz art. 49

Uwagi:

Projektowana ustawa wymaga dalszych zmian w zakresie uprawnień nadzorczych Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (dalej „Komisja”), tak, aby uprawnienia nadzorcze Komisji odpowiadały uprawnieniom, które dla organów właściwych przewiduje unijny Akt o sztucznej inteligencji.

Unijny Akt o sztucznej inteligencji jest rozporządzeniem, które jest bezpośrednio stosowane (tj. nie wymaga implementacji) na terytorium Rzeczypospolitej Polskiej. Oznacza to m.in., że ustawa nie może powtarzać ani przepisywać przepisów rozporządzenia, tym bardziej przepisy ustawy nie mogą być sprzeczne ani nie mogą modyfikować przepisów rozporządzenia. Zatem projektowana ustawa powinna wskazywać organ (Komisja), który w polskich warunkach będzie organem właściwym odpowiedzialnym za nadzór nad rynkiem i egzekwowanie przepisów i to jest podstawowym celem i zadaniem ustawy. Tak wskazany organ będzie dysponował uprawnieniami wskazanymi w unijnym rozporządzeniu o systemach sztucznej inteligencji. Jednocześnie ustawa nie powinna dawać krajowemu organowi kompetencji i uprawnień innych, niż przewidziane w unijnym akcie w sprawie sztucznej inteligencji, nie może też modyfikować uprawnień wynikających z unijnego rozporządzenia. Niestety tych warunków nie spełniają przepisy projektowanej ustawy dotyczące:

1. Uprawnienia Komisji do wydania decyzji nakazującej operatorowi tego systemu zaprzestanie stosowania lub wycofanie systemu sztucznej inteligencji w przypadku stwierdzenia przez Komisję, że system sztucznej inteligencji stwarza bezpośrednie

member of



BUSINESSatOECD

member of



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

ryzyko zagrożenia dla życia, zdrowia, bezpieczeństwa lub praw podstawowych osób fizycznych (art. 49 ust. 2 projektowanej ustawy).

2. Uprawnienia Komisji do nakazania, w drodze postanowienia, nakazania zablokowania lub uniemożliwienia uzyskania dostępu przez użytkowników końcowych do systemu lub też do elementów będących przedmiotem ostrzeżenia lub wycofanie z rynku lub użytku systemu w całości lub też części lub elemencie, którego dotyczy ostrzeżenie (art. 47 projektowanej ustawy).

W tym miejscu należy zauważyć, że unijne rozporządzenie w sprawie systemów sztucznej inteligencji wprost stanowi (na co zwracał uwagę również Minister do spraw Unii Europejskiej w piśmie z uwagami do Projektu Ustawy), że do systemów sztucznej inteligencji objętych rozporządzeniem stosuje się również przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów (art. 74 ust. 1 rozporządzenia w sprawie systemów sztucznej inteligencji). Jak wynika z motywu 156 rozporządzenia w sprawie systemów sztucznej inteligencji organy nadzoru rynku powinny mieć wszystkie uprawnienia w zakresie egzekwowania wymogów i obowiązków ustanowione w rozporządzeniu:

- w sprawie systemów sztucznej inteligencji (2024/1689); oraz
- w sprawie nadzoru rynku i zgodności produktów (2019/1020).

Zatem przepisy tych dwóch rozporządzeń określają bezpośrednio (bez potrzeby implementacji) jakimi uprawnieniami i narzędziami władczymi dysponuje organ właściwy państwa członkowskiego, czyli Komisja w przypadku Polski. Ustawą nie można poszerzać ani modyfikować uprawnień organu właściwego wynikających bezpośrednio z tych rozporządzeń. Ustawa nie powinna również powtarzać ani przepisywać tych uprawnień, tym bardziej jeśli przy okazji następuje ich modyfikacja w stosunku do tego, co wynika z unijnych rozporządzeń.

Środki nadzoru rynku, które powinny przysługiwać organom nadzoru, zostały określone m.in. w art. 16 rozporządzenia w sprawie nadzoru rynku i zgodności produktów (2019/1020), który stanowi, że jeżeli organ nadzoru rynku ustali, że system sztucznej inteligencji stwarza ryzyko dla zdrowia lub bezpieczeństwa użytkowników, lub nie jest zgodny z rozporządzeniem w sprawie systemów sztucznej inteligencji to organ żąda niezwłocznie od właściwego podmiotu gospodarczego podjęcia odpowiednich i proporcjonalnych działań naprawczych w celu doprowadzenia do usunięcia niezgodności lub wyeliminowania ryzyka w określonym przez ten organ terminie. Zgodnie z art. 16 ust. 3 rozporządzenia w sprawie nadzoru rynku i zgodności produktów działanie naprawcze wymagane od podmiotu gospodarczego może obejmować między innymi:

member of



member of



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

- 1) zapewnienie zgodności produktu z przepisami, w tym poprzez skorygowanie formalnej niezgodności, jak określono w obowiązującym unijnym prawodawstwie harmonizacyjnym, lub poprzez zapewnienie, aby produkt nie stwarzał już ryzyka;
- 2) uniemożliwienie udostępniania produktu na rynku;
- 3) natychmiastowe wycofanie produktu z obrotu lub odzyskanie produktu oraz powiadomienie opinii publicznej o stwarzanym przez ten produkt ryzyku;
- 4) zniszczenie produktu lub uczynienie go niezdatnym do użytku w inny sposób;
- 5) umieszczenie na produkcie odpowiednich, jasno sformułowanych i zrozumiałych ostrzeżeń o ryzyku, jakie może on stwarzać, w języku lub językach określonych przez państwo członkowskie, w którym dany produkt jest udostępniany na rynku;
- 6) określenie z góry warunków, na jakich dany produkt może być udostępniany na rynku;
- 7) natychmiastowe powiadomienie narażonych na ryzyko użytkowników końcowych
- 8) w stosownej formie, w tym za pomocą specjalnych ostrzeżeń w języku lub językach określonych przez państwo członkowskie, w którym dany produkt jest udostępniany na rynku.

Ponadto, art. 79 rozporządzenia w sprawie systemów sztucznej inteligencji (2024/1689) zawiera dedykowaną procedurę wobec systemów AI stwarzających ryzyko dla zdrowia i bezpieczeństwa lub praw podstawowych, dając organom właściwym kompetencję do żądania od operatora podjęcia wszelkich odpowiednich działań naprawczych, aby zapewnić zgodność tego systemu AI z wymogami albo wycofać ten system z rynku lub z użytku.

Z powyższego jednoznacznie wynika, rozporządzenie w sprawie systemów sztucznej inteligencji (2024/1689) oraz rozporządzenie w sprawie nadzoru rynku i zgodności produktów (2019/1020) razem dają uprawnionym organom szereg uprawnień w przypadku stwierdzenia, że system sztucznej inteligencji stwarza ryzyko dla zdrowia lub bezpieczeństwa użytkowników, w tym uprawnienie do uniemożliwienia udostępniania produktu na rynku oraz uprawnienie do żądania wycofania produktu z obrotu. Nie ma zatem potrzeby, aby projektowana ustawa dawała te sama albo bardzo podobne uprawnienia Komisji, skoro Komisja będzie dysponowała tymi kompetencjami bezpośrednio na gruncie analizowanych rozporządzeń. Krajowe przepisy w tym zakresie są nie tylko zbędne, ale wręcz stanowią naruszenie analizowanych rozporządzeń, gdyż dla takich samych przesłanek konstruują kompetencje Komisji odmiennie niż przepisy analizowanych rozporządzeń.

Wracając na grunt projektowanej ustawy należy wskazać, że art. 49 ust. 2 projektu ustawy stanowi, że w przypadku stwierdzenia przez Komisję, że system sztucznej inteligencji stwarza bezpośrednie ryzyko zagrożenia dla życia, zdrowia, bezpieczeństwa lub praw podstawowych osób fizycznych, Komisja może wydać decyzję nakazującą operatorowi tego systemu zaprzestanie stosowania lub wycofanie systemu. Dostrzegamy, że zakres przedmiotowy tego przepisu został zmieniony (w stosunku do wcześniejszych wersji projektowanej ustawy)

przez usunięcie z przepisu kontrowersyjnych przesłanek odnoszących się do emocji i wyborów (co jest zmianą bardzo dobrą), niemniej jednak nie jest to zmiana wystarczająca, gdyż - **jak już wcześniej zgłaszaliśmy - art. 49 ust. 2 powinien zostać usunięty z projektu ustawy w całości**, gdyż w obecnym brzmieniu przepis ten powiela uprawnienia, które Komisji będą przysługiwały bezpośrednio na gruncie rozporządzeń UE, na domiar złego trochę modyfikując ustawą uprawnienia wynikające z rozporządzenia (hierarchia i kolejność uprawnień i zasady ich stosowania nie są tożsame na gruncie projektowanej ustawy i rozporządzenia). Z tych względów art. 49 ust. 2 powinien zostać w całości usunięty z projektu ustawy, co w żaden sposób nie uszczupli prerogatyw Komisji, gdyż te Komisji będą przysługiwały bezpośrednio na gruncie analizowanych rozporządzeń.

Z projektu ustawy usunięty powinien być również art. 47 projektu ustawy, jeśli nie w całości to usunięty powinien być przynajmniej ustęp 4 tego artykułu, w zakresie w jakim przekształca niewładczy mechanizm „ostrzeżenia” we władcze rozstrzygnięcie, niewymagające od organu udowodnienia naruszenia. Analogicznego uprawnienia (tj. ostrzeżenia, które może stać się wiążącym nakazem) nie ma w rozporządzeniach unijnych, określających uprawnienia organów właściwych. Ponadto, pomimo naszych wcześniejszych uwag przepis art. 47 jest błędnie skonstruowany, gdyż „ostrzeżenie” powinno być narzędziem miękkim, niewładczym, czyli takim, za którego niewykonanie nie może grozić kara i nie może być nakazem (bo przestaje być ostrzeżeniem). Zgodnie z art. 47 ust. 1 i 2 projektowanej ustawy w przypadku ostrzeżenia Komisja nie musi udowodnić naruszenia (wystarczy „uzasadnione podejrzenie”) i nie musi wydawać decyzji administracyjnej (wystarczy postanowienie). I taką funkcję spełnia ostrzeżenie opisane w ust. 1 -3 art. 47 projektowanej ustawy. Niestety ustęp czwarty analizowanego art. 47 zamienia ostrzeżenia w instrument władczy, stanowiąc, że jeśli strona nie wykona „ostrzeżenia”, to Komisja będzie mogła m.in. nakazać stronie zablokowanie lub uniemożliwienie uzyskania dostępu przez użytkowników końcowych do systemu lub też do elementów będących przedmiotem ostrzeżenia lub wycofanie z rynku lub użytku systemu w całości lub też części lub elemencie, którego dotyczy ostrzeżenie - wciąż w drodze postanowienia (a nie decyzji administracyjnej) i wciąż bez konieczności udowodnienia przez Komisję, że doszło do naruszenia (wystarczy pierwotne „uzasadnione podejrzenie”). Takie „ostrzeżenie” nie jest ostrzeżeniem, jest natomiast mechanizmem władczym, do którego zastosowania konieczne powinno być udowodnienie naruszenia oraz wydanie decyzji administracyjnej. Problem dosyć dobrze obrazuje wewnętrzna rozbieżność w ramach samego projektu ustawy, gdzie z jednej strony art. 47 ust. 4 pkt 1) daje Komisji możliwość zablokowania lub uniemożliwienia dostępu postanowieniem i na podstawie uzasadnionego podejrzenia, podczas gdy art. 49 ust. 2 projektowanej ustawy dla analogicznego nakazu wymaga wydania decyzji administracyjnej (i udowodnienia naruszenia). Podsumowując, przepisy dotyczące ostrzeżeń powinny zostać usunięte z projektowanej ustawy (gdyż nie mają podstawy w rozporządzeniach UE), a co najmniej usunięte powinny zostać te przepisy, które „ostrzeżenia” zamieniają we władczy instrument, niewymagający udowodnienia naruszenia ani wydania decyzji administracyjnej.

5. Art. 110

Uwagi:

Bardzo pozytywnie należy ocenić zmianę wprowadzoną w artykule 110 najnowszej wersji projektu Ustawy – polegającą na dodaniu do przepisu punktu 2:

Art. 110. *Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem:*

- 1) *art. 105 - 107, które wchodzi w życie z dniem następującym po dniu ogłoszenia;*
- 2) *przepisów rozdziału 6, które wchodzi w życie 2 sierpnia 2026 r.*

Przepis ten wyjaśnia wątpliwość dotyczącą relacji daty wejścia w życie obowiązku określonego w art. 73 AI Act wynikającej z art. 113 AI Act – czyli 2 sierpnia 2026 r. z datą wejścia w życie ustawy, w zakresie przepisów odnoszących się do tego obowiązku, określonych w Rozdziale 6.

Należy jednak rozważyć, czy analogiczny zapis, jak w dodanym punkcie 2) art. 110 projektu Ustawy nie powinien odnosić się także do pozostałych obowiązków, uprawnień, które zgodnie z art. 113 AI Act wchodzi w życie w dniu 2 sierpnia 2026 r., jak np. określone w art. 85 prawo do wniesienia skargi do organu nadzoru rynku – o którym mowa w rozdziale 4 projektu Ustawy.

Wprawdzie uzupełniona treść uzasadnienia projektu Ustawy wskazuje, że:

„Jednoczenie wyjaśnić należy, że w zakresie spraw uregulowanych:

- 1) *w rozdziale III sekcje 1-3 i sekcja 5, rozdziale IV, rozdziale VI, rozdziałach VIII-XI, z wyłączeniem art. 78, oraz w zakresie spraw uregulowanych w art. 101 rozporządzenia z 2024/1689, przepisy ustawy będą obowiązywały od 2 sierpnia 2026 r.;*
- w art. 6 ust. 1 rozporządzenia 2024/1689 i odpowiadających mu obowiązków ustanowionych w tym rozporządzeniu, przepisy ustawy będą obowiązywały od 2 sierpnia 2027 r.*

Wskazane terminy wynikają wprost z art. 113 rozporządzenia 2024/1689.”

jednak wynika to tylko z treści uzasadnienia, do którego po zakończeniu procesu legislacyjnego obywatele nie będą sięgać. Lektura zaś treści samej ustawy, w tym obecnej propozycji brzmienia art. 110 sugeruje, że wszystkie przepisy ustawy – także te odwołujące do przepisów Rozporządzenia wchodzi w życie w terminie 14 dni od ogłoszenia ustawy, tylko z jednym wyjątkiem – Rozdziału 6.

Proponowane rozwiązanie:

member of



BUSINESS@OECD

member of

BUSINESSEUROPE

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

Z tego względu rekomendujemy, aby przepis art. 6 został uzupełniony o powyższy zapis z treści uzasadnienia projektu Ustawy bądź o inne odpowiednie zapisy, pozwalające wprost z treści samej ustawy wyczytać terminy wejścia w życie jej poszczególnych przepisów.

6. Obowiązki związane ze zgłaszaniem poważnych incydentów

Wyrażamy zaniepokojenie nowymi zapisami dotyczącymi obowiązków zgłaszania poważnych incydentów zaistniałych w związku z wykorzystaniem systemów sztucznej inteligencji.

Zgodnie z proponowanym brzmieniem ustawy, obowiązek niezwłocznego zgłoszenia Komisji incydentu stwarzającego poważne ryzyko ciąży **nie tylko na dostawcy systemu AI wysokiego ryzyka, lecz także na podmiocie stosującym taki system.**

Odwołując się do definicji zawartej w Rozporządzeniu dot. sztucznej inteligencji (AI Akt), „poważny incydent” oznacza zdarzenie lub nieprawidłowe działanie systemu AI, które bezpośrednio lub pośrednio skutkuje przynajmniej jednym z następujących efektów:

- śmiercią lub poważnym uszczerbkiem na zdrowiu osoby;
- poważnym i nieodwracalnym zakłóceniem funkcjonowania infrastruktury krytycznej;
- naruszeniem obowiązków wynikających z prawa Unii mających na celu ochronę praw podstawowych;
- poważną szkodą na mieniu lub środowisku.

W kontekście dodatkowych obowiązków dla stosujących istotny jest pkt. 3 powyżej, ponieważ powoduje najwięcej problemów interpretacyjnych i wątpliwości jak go stosować w praktyce. Katalog obowiązków związanych z ochroną praw podstawowych jest bowiem bardzo szeroki – obejmuje m.in. prawo do ochrony prywatności i danych osobowych (naruszenie np. nieuprawnione ujawnianie danych osobowych), prawo do równego traktowania i niedyskryminacji (naruszenie np. poprzez uprzedzenia algorytmiczne), prawo do pracy i sprawiedliwych warunków pracy (naruszenie np. przez nierównego traktowanie kandydatów przez AI); prawo do ochrony zdrowia (naruszenie np. przez błędy w systemach AI wykorzystywanych w diagnostyce lub leczeniu medycznym). Tym samym, potencjalny incydent może dotyczyć nie tylko przypadków blackoutu czy śmierci, ale także wielu innych sytuacji, w których działanie systemu AI może wpływać na prawa jednostki. Innymi słowy, w przypadku naruszeń obowiązków wynikających z prawa Unii nie ma znaczenia skala zdarzenia – w definicji poważnego incydentu w przypadku naruszeń obowiązków wynikających z prawa Unii mających na celu ochronę praw podstawowych nie wskazano bowiem, że naruszenie musi mieć charakter poważny. Oznacza to, że w praktyce **każde tj. zwykłe lub, nawet nieznaczne naruszenie tych obowiązków, może skutkować koniecznością zgłoszenia incydentu** także przez podmiot stosujący system AI wysokiego

member of



member of



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenberg 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

ryzyka. Z pewnością pojawią się wątpliwości, niepewność prawna i konieczność wyboru czy akceptować formalne ryzyko, czy zgłaszać “na wszelki” wypadek czy w ogóle zrezygnować z inicjatywy działania z powodu ryzyka incydentu.

Przykładowo, drobny błąd w procesie rekrutacyjnym, gdzie stosowano narzędzie high- risk AI, taki jak błędna selekcja kandydatów na podstawie CV, może pociągać za sobą obowiązek formalnego zgłoszenia incydentu tylko dlatego, że “podmiot stosujący” wskazano w nowym brzmieniu ustawy. O ile zgadzamy się, że naruszenia praw podstawowych w skutek wykorzystania technologii w ogóle nie powinny mieć miejsca, o tyle jesteśmy zdania, że na dostawcy systemów i stosujących nie powinny spoczywać jednakowe obowiązki w zakresie odpowiedzialności i procedury informowania o zdarzeniach.

Warto podkreślić, że sam AI Akt w art. 73 ust. 1 nakłada obowiązek zgłaszania incydentów **wyłącznie na dostawców systemów AI wysokiego ryzyka**, którzy wprowadzają je do obrotu na rynku Unii Europejskiej. Art. 26 ust. 5 AI Aktu mówi co prawda, że w przypadku gdy podmioty stosujące stwierdziły wystąpienie poważnego incydentu, natychmiast informują o tym incydencie najpierw dostawcę, a następnie importera lub dystrybutora oraz odpowiednie organy nadzoru rynku. Jednak ich obowiązek polega jedynie na informowaniu odpowiednich podmiotów, nie zaś na przechodzeniu formalnej procedury zgłaszania incydentu. Dopiero w momencie, gdy podmiot stosujący nie jest w stanie skontaktować się z dostawcą, odpowiednio stosuje się art. 73. Widocznym jest więc, że AI Akt nie zrównuje obowiązków dostawców i podmiotów stosujących i zapewnia „kaskadowość” zgłaszania poważnych incydentów – w pierwszej kolejności odpowiedzialny jest dostawca, a dopiero w przypadku jego braku – stosujący. Z tego względu, w naszej ocenie najnowszy projekt ustawy wdrażającej AI Akt, ujednolicając obowiązki dostawcy i stosującego, zawiera w omawianym zakresie **istotne uproszczenie**, które może nosić znamiona „goldplatingu”.

Biorąc pod uwagę zakres wymaganych informacji (do których sami stosujący mogą nie mieć dostępu), a także złożoność całej procedury, realizacja takiego obowiązku może generować znaczną biurokrację i trudności dla szerokiego grona podmiotów, w szczególności dla małych i średnich firm wykorzystujących niewielkie systemy AI np. w rekrutacji.

W związku z powyższym **rekomendujemy, by nie zrównywać obowiązków dostawców i podmiotów stosujących systemy wysokiego ryzyka oraz usunąć obowiązek zgłaszania poważnych incydentów przez podmioty stosujące** z zapisów polskiej ustawy wdrażającej AI Akt lub wprowadzić **adekwatne różnicowanie obowiązków** poprzez uwzględnienie “kaskadowej” odpowiedzialności, podobnej do tej przewidzianej w samym AI Akcie.

Ponadto, projekt przewiduje możliwość przekazywania tajemnic prawnie chronionych, w tym tajemnicy przedsiębiorstwa, innym właściwym organom. Takie rozwiązanie wydaje się **nadmiarowe w stosunku do postanowień rozporządzenia AI Akt**, zwłaszcza jeśli zgłaszanie

incydentów miałyby dotyczyć także podmiotów stosujących systemy wysokiego ryzyka – co oznaczałoby znaczne ryzyko naruszenia poufności i tajemnicy przedsiębiorstwa. Dodatkowo, w treści tego zapisu znajduje się nieścisłość – organy właściwe, do których wydaje się odnosić ustawodawca w art. 72 ust. 3 wymienione są nie w ust. 2, a w ust. 1 omawianego artykułu.

KL/407/139/ET/2025

member of



BUSINESSatOECD

member of

BUSINESSEUROPE

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy