

Warszawa, dnia 26 marca 2025 r.

Pan Michał Gramatyka
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 konsultacjach publicznych projektu ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w Internecie.

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. Członkami AmCham są w szczególności wszyscy najważniejsi amerykańscy inwestorzy działający w sektorze nowych technologii, w tym najwięksi dostawcy usług cyfrowych. Co za tym idzie, kwestie standardów bezpieczeństwa w Internecie należą do najważniejszych obszarów naszego zainteresowania.

Poniższe stanowisko jest rozwinięciem uwag zgłoszonych już przez przedstawiciela AmCham w trakcie wysłuchania publicznego ustawy, które odbyło się 12 marca w siedzibie Ministerstwa Cyfryzacji. Bardzo dziękujemy również za możliwość udziału w tej formie konsultacji ustawy i doceniamy otwartość ministerstwa na różne możliwości uwzględniania opinii sektora prywatnego w toczącym się procesie legislacyjnym.

Poniżej przekazujemy stanowisko AmCham do przedmiotowego projektu:

AmCham jednoznacznie pozytywnie odnosi się do inicjatyw zmierzających do poprawy poziomu bezpieczeństwa dzieci i młodzieży online. Jesteśmy przekonani, że zaproponowany przez Ministerstwo Cyfryzacji projekt ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w Internecie może stanowić istotny krok w stronę bardziej skutecznego zwalczania negatywnych skutków niekontrolowanego dostępu do treści o charakterze pornograficznym. Jednocześnie zwracamy uwagę na niektóre aspekty proponowanych regulacji, które mogą prowadzić do konfliktów ustawy z prawem unijnym lub nieproporcjonalnie obniżyć poziom pewności prawnej dla przedsiębiorców świadczących usługi cyfrowe.

A. Uwagi ogólne

1. Ryzyka prawne związane z przewidywaną w ustawie procedurą blokowania dostępu do stron internetowych

Proponowana obecnie treść przepisów prowadzi do poważnego ryzyka dla funkcjonowania dostawców treści online, których działalność może zostać zablokowana na podstawie uznaniowej decyzji administracyjnej. Zastosowanie procedury odwoławczej po wpisie do rejestru domen umożliwiających dostęp do treści pornograficznych np. sądowo-administracyjnej, nie jest rozwiązaniem wystarczającym, ze względu na długotrwałość takiego postępowania. Jednocześnie należy podkreślić konsekwencje prawne, w tym potencjalną odpowiedzialność odszkodowawczą Skarbu Państwa w sytuacji, gdy dojdzie do uchylecia decyzji o wpisaniu domeny do rejestru.

1.1 Zdiagnozowane ryzyka prawne

Procedura dotycząca dokonania wpisu do rejestru nazw domen umożliwiających dostęp do treści pornograficznych bez uprzedniej weryfikacji wieku w proponowanej postaci rodzi ryzyko wykorzystania jej do ograniczenia wolności wypowiedzi. Jako przykład można wskazać zgłoszenie, które dotyczy jednego materiału audiowizualnego, który zostanie oceniony przez Prezesa UKE jako materiał zawierający treści pornograficzne. W takiej sytuacji zgodnie z wymogami projektowanych przepisów Prezes UKE dokonuje zgłoszenia do rejestru. Literalna treść przepisu wskazuje na

obowiązek dokonania takiego zgłoszenia przez Prezesa UKE, bez względu na zakres naruszenia. Innymi słowy jeden materiał o charakterze pornograficznym stanowi podstawę do wpisania do rejestru całego serwisu udostępniającego treści online. W ten sposób łatwo może dojść do sytuacji, w której przypadkowa scena „o charakterze pornograficznym” w jednym z materiałów audiowizualnych, zostanie wykorzystana do „zablokowania” całej domeny, w tym innych treści, które nie mają charakteru treści pornograficznych.

Procedura przewidziana w projekcie ustawy, opierająca się na „automatyzmie” wskazanym wyżej, może w szczególności być wykorzystana instrumentalnie przez konkurujące ze sobą podmioty świadczące usługi. Zgłoszenie wskazujące choćby na jeden materiał o charakterze pornograficznym, będzie skutkować wpisem do rejestru. W ten sposób czasowo lub trwale konkurencyjna domena będzie niedostępna.

1.2 Propozycja alternatywnego rozwiązania

Alternatywne, mniej represyjne i bardziej proporcjonalne rozwiązanie mogłoby opierać się na wyróżnieniu naruszeń dotyczących udostępniania treści pornograficznych w oparciu o zakres lub intensywność udostępniania tych treści, a także wprowadzenie dodatkowych gwarancji dla usługodawców. Za podstawowy model w przypadku powstania podejrzenia udostępniania treści pornograficznych bez weryfikacji wieku należałoby uznać wynikający z aktu o usługach cyfrowych mechanizm *notice and take down*. W ten sposób usługodawca uzyskalby możliwość samodzielnego uniemożliwienia lub odpowiedniego ograniczenia dostępu do takiej treści.

Dopiero gdyby zgłoszenie dokonane zgodnie z procedurą stosowaną przez usługodawcę, dokonane przez jakiegokolwiek podmiot wskazany w art. 7 Projektu, nie przyniosłoby skutku lub usługodawca odmówiłby uniemożliwienia lub ograniczenia dostępu, Prezesa UKE, z zachowaniem praw usługodawcy do wyrażenia swojego stanowiska, mógłby nakazać uniemożliwienie dostępu do konkretnej treści. Jeśli usługobiorca nie podporządkowałby się temu nakazowi w terminie, Prezes UKE zgłaszałby domenę do rejestru.

Odmienne uregulowana powinna zostać sytuacja domen, które udostępniają treści oczywiście pornograficzne¹ w znacznej ilości². Nie chodzi zatem o pojedyncze materiały (pliki), które stanowią znikomy procent lub promil całości treści udostępnionych w danej domenie, lecz o takie domeny, których zawartość w większości stanowią materiały o charakterze oczywiście pornograficznym. Jeśli zawartość domeny w sposób oczywisty narusza prawo w zakresie udostępniania znacznych ilości materiałów treści pornograficznych, to uzasadnione może być rozwiązanie prawne, które opiera się na bezpośrednim zgłoszeniu takiej domeny do Prezesa UKE z pominięciem procedury *notice and take down*. Prezes UKE powinien w takiej sytuacji wezwać usługodawcę do uniemożliwienia dostępu do treści pornograficznych małoletnim lub – zgodnie z intencją projektu – umożliwienia takiego dostępu wyłącznie osobom pełnoletnim, a w razie bezskuteczności takiego wezwania, zgłosić domenę do rejestru.

2. Definicja pornografii

Mimo przyjęcia do wiadomości argumentów przedstawionych podczas wysłuchania publicznego, pozostajemy na stanowisku, że wprowadzenie nawet ogólnej definicji treści pornograficznych podniosłoby poziom pewności prawa i zmniejszyło ryzyko nieracjonalnie rozszerzającej wykładni tego pojęcia. Orzecznictwo sądowe, głównie w sprawach karnych wypracowało zbiór kryteriów pomocnych przy ocenie tego rodzaju treści, ale nadal pozostają wątpliwości co do stosowania tych kryteriów oraz ich dokładnej treści. Na potrzeby projektu ustawy o ochronie małoletnich można

¹ Oczywiście naruszenie prawa jest zdefiniowane w orzecznictwie Sądu Najwyższego jako naruszenia, „widoczne od razu, przy wykorzystaniu podstawowej wiedzy prawniczej, bez potrzeby głębszej analizy”.

² Pojęcie znacznej ilości (lub znacznych rozmiarów) jest używane w różnych aktach prawnych. Może być ono używane jako pojęcie niedookreślone. Można także zdefiniować to pojęcie (podobnie jak to zostało uczynione w Kodeksie karnym, posługującym się pojęciem „mienia znacznej wartości” (art. 115 § 5 kk). Gdyby ustawodawca zdecydował się zastosowanie definicji pojęcia znacznej ilości materiałów pornograficznych, to można zaproponować, aby zakresem tego pojęcia objąć takie sytuacje, gdy w ramach tej samej domeny udostępnionych jest co najmniej określony % materiałów o charakterze oczywiście pornograficznym np. do 25%. Aby ograniczyć ryzyko obejścia prawa (polegające na umieszczeniu materiałów oczywiście pornograficznych w katalogu „wypełnionym w 90%” przez materiały nie będące pornograficznymi) można zastosować także kryterium ilościowe np. 100 materiałów oczywiście pornograficznych. Jeśli którykolwiek z parametrów będzie spełniony, należy uznać, że domena zawiera znaczną ilość takich treści.

zaproponować zastosowanie dodatkowych kryteriów, które mogą być pomocne, bez uszczerbku dla wypracowanego dotychczas stanowiska judykatury. Pozwoliłoby to na lepsze ukierunkowanie decyzji podejmowanych przez organy stosowania prawa i zapobiegło potencjalnemu stosowaniu ustawy niezgodnemu z intencjami projektodawcy.

Ocena tego czy dane treści dostawcy są treściami pornograficznymi nie powinna być indywidualną interpretacją podmiotu kontrolującego – powinna się opierać na konkretnych kryteriach oceny wraz z uzasadnieniem, tak aby ocena ta nie miała negatywnego wpływu na działania dostawcy np. poprzez zablokowanie usługi na czas prowadzenia postępowania odwoławczego w sytuacji, gdy zasady i kryteria nie są jasno określone.

3. Zgodność z prawem Unii Europejskiej

Za kluczowo istotną uznajemy spójność projektu z obowiązującym prawem unijnym, co zapewni skuteczność i przejrzystość nowych regulacji i uniknie kreowania niepotrzebnych barier dla usługodawców działających na rynku wewnętrznym. Rekomendujemy ponowną weryfikację projektu pod kątem potencjalnych konfliktów, zwłaszcza wobec faktu, że w ramach procesu legislacyjnego powinien zostać spełniony obowiązek wynikający z dyrektywy 2015/1535 (tzw. procedura TRIS), tj. wymóg zgłaszania Komisji Europejskiej wszelkich projektów przepisów technicznych dotyczących produktów i usług społeczeństwa informacyjnego przed ich przyjęciem. Niezgłoszenie projektu lub przyjęcie przepisów sprzecznych z prawem UE może stanowić naruszenie zobowiązań państwa członkowskiego, co rodzi ryzyko opóźnień w stosowaniu nowych przepisów i wzrostu niepewności prawnej dla wszystkich podmiotów objętych regulacją.

W szczególności zwracamy uwagę na konieczność analizy projektu pod następującymi względami:

- 1) Akt o usługach cyfrowych zawiera przepisy odnoszące się do osób małoletnich. Jak stwierdzono w motywie 71 "ochrona małoletnich jest ważnym celem polityki Unii Europejskiej. [...] Dostawcy platform internetowych, z których korzystają małoletni, powinni wprowadzić odpowiednie i proporcjonalne środki w celu ochrony małoletnich, na przykład poprzez domyślne, w stosownych przypadkach, projektowanie swoich interfejsów internetowych lub ich części z zachowaniem najwyższego poziomu prywatności, bezpieczeństwa i ochrony małoletnich, a także poprzez przyjmowanie norm ochrony małoletnich lub stosowanie kodeksów postępowania służących ochronie małoletnich. Kwestia ochrony małoletnich została szczegółowo uregulowana w art. 14 (Regulamin), 28 (Ochrona małoletnich w Internecie), 34 (Ocena ryzyka) i 35 (Łagodzenie ryzyka). W tym świetle konieczna wydaje się dodatkowa weryfikacja przepisów projektowanej ustawy, szczególnie tych wykraczających poza jej zasadniczy cel, tj. ochronę małoletnich przed treściami pornograficznymi, pod kątem zgodności z DSA. Szczególne wątpliwości mogą w tym zakresie budzić obowiązki dotyczące niezdefiniowanych w ustawie „treści nieodpowiednich” (art. 1 ust. 1 pkt 1) oraz nowe obowiązki oceny ryzyka (art. 3).

Komisja Europejska uważa ochronę małoletnich w Internecie za jeden z głównych celów aktu o usługach cyfrowych i w przeszłości krytykowała już ustawodawstwo krajowe w tej dziedzinie jako potencjalne naruszenie bezpośredniego stosowania Aktu. Na przykład, KE ostro skrytykowała dwie francuskie ustawy, które m. in. nakładały obowiązki związane z bezpieczeństwem małoletnich na usługodawców niezależnie od miejsca prowadzenia przez nich działalności, co narusza obowiązywanie DSA jako jednolicie i bezpośrednio stosowanego prawa europejskiego. Przez wprowadzanie dodatkowych obowiązków, krajowe inicjatywy ustawodawcze mogą prowadzić do fragmentaryzacji jednolitego rynku cyfrowego.

Akt o usługach cyfrowych w pełni harmonizuje warunki świadczenia usług pośrednich na rynku wewnętrznym, w celu zapewnienia bezpiecznego i zaufanego środowiska internetowego, przeciwdziałania zagrożeniom społecznym i rozpowszechnianiu nielegalnych treści online. W ramach aktu zapisane w karcie praw podstawowych prawa są skutecznie chronione, przy jednoczesnym wspieraniu innowacyjności. W związku z tym państwa członkowskie co do zasady nie powinny przyjmować ani wprowadzać dodatkowego, lokalnego prawodawstwa pokrywającego się z zakresem DSA.

- 2) W szczególności, projekt ustawy powinien być zgodny z przewidywanymi wytycznymi Komisji Europejskiej dotyczącymi art. 28 DSA opartymi na Europejskiej strategii na rzecz lepszego Internetu dla dzieci (BIK+), które najprawdopodobniej rozszerzą obowiązek przeprowadzania oceny ryzyka pod kątem ochrony małoletnich na wszystkie usługi cyfrowe — nie tylko na bardzo duże platformy internetowe (VLOPs). Wprowadzenie dodatkowych krajowych wymogów, które wykraczają poza DSA, mogłoby naruszyć spójność rynku wewnętrznego. W przypadku utrzymania obowiązku oceny ryzyka, istotne jest, aby projekt ustawy umożliwiał uznanie oceny przeprowadzonej na podstawie DSA za równoważną ze spełnieniem obowiązku wynikającego z ustawy;
- 3) Należy wziąć pod uwagę obowiązujące już przepisy dotyczące ochrony małoletnich w Internecie wynikające z prawa europejskiego, w tym z dyrektywy o audiowizualnych usługach medialnych (AVMS), która obejmuje platformy udostępniania wideo oraz usługi na żądanie. Przepisy krajowe nie powinny wykraczać poza wymagania wynikające z tej dyrektywy w zakresie jej stosowania, aby uniknąć rozbieżności pomiędzy krajami członkowskimi UE i zapewnić jednolitość regulacyjną na rynku wewnętrznym;
- 4) Zasada kraju pochodzenia, wynikająca z art. 3 dyrektywy o handlu elektronicznym, ogranicza prawo państw członkowskich do nakładania dodatkowych, lokalnych obowiązków na dostawców usług z siedzibą w innym kraju UE. Warto przy tym podkreślić, że przestrzeganie tej zasady nie zwalnia usługodawców z odpowiedzialności za ochronę dzieci w Internecie. Przykład Irlandii, gdzie regulator CNAM wprowadził kompleksowe ramy ochrony dzieci online zgodne z prawem unijnym, pokazuje, że jest to możliwe bez naruszania zasady COO. W szczególności zwracamy uwagę na konieczność weryfikacji poszczególnych postanowień ustawy pod względem testów konieczności, proporcjonalności oraz spełniania kryterium podejmowania przeciw określonej usłudze społeczeństwa informacyjnego, która narusza lub faktycznie i poważnie grozi naruszeniem celów określonych w dyrektywie.

4. Treści szkodliwe

Za niecelowe uznajemy włączenie do projektu przepisów odnoszących się do pojęcia „treści szkodliwych”. Zdecydowana większość uzasadnienia oraz przepisów merytorycznych ustawy dotyczy celu zgodnego z publicznymi deklaracjami projektodawcy, tj. walki z wystawianiem małoletnich na ryzyko kontaktu z treściami pornograficznymi. Wprowadzenie dodatkowych regulacji odwołujących się do pojęcia „treści szkodliwych” nie tylko nie sprzyja realizacji tego słusznego i niekontrowersyjnego celu, ale także radykalnie obniża poziom pewności prawnej dla dostawców usług elektronicznych. Pojęcie „treści szkodliwych” nie zostało zdefiniowane w projekcie i nie ma jasno określonej treści wypracowanej w orzecznictwie lub doktrynie. Może być ono podatne na bardzo szeroką interpretację zależną od światopoglądu i przekonań politycznych. Odwołanie do treści szkodliwych i oparty na nim mechanizm obowiązkowej oceny ryzyka zwiększa w końcu ryzyko niezgodności projektowanej ustawy z regulacjami unijnymi, w szczególności z aktem o usługach cyfrowych.

Naszym zdaniem, ustawodawca powinien skupić się na dostawcach usług elektronicznych, którzy umożliwiają dostęp do treści pornograficznych, tym samym konsekwentnie zarysowując zakres przepisów w całym tekście ustawy. Wprowadzenie do ustawy terminu „treści szkodliwe” tworzy wyraźne przecięcia z DSA i wprowadza wymogi, które wykraczają poza ten akt, zaprzeczając idei jednolitego rynku. Przepisy art. 3 dotyczące oceny ryzyka i szkodliwych treści wydają się nachodzić na zakres stosowania podobnych przepisów dotyczących VLOP w DSA (w szczególności art. 34-35) przy jednoczesnym ustaleniu wymagań wyższych niż w unijnym rozporządzeniu. Ponadto, przepisy przyznają UKE szerokie uprawnienia, w tym do przeprowadzania kontroli i wydawania nakazów. Artykuł 14 upoważnia również NASK do „analizowania zagrożeń związanych z dostępem małoletnich do szkodliwych treści w Internecie i publikowania komunikatów w tym zakresie na swojej stronie internetowej”. Również to uprawnienie jest sformułowane bardzo szeroko, między innymi poprzez użycie terminu „szkodliwe treści”. Istnieje ryzyko, że organy krajowe będą wkraczać w uprawnienia Komisji Europejskiej, która jest organem regulacyjnym w zakresie stosowania DSA.

W przypadku, gdyby projektodawca zdecydował się zachować obowiązek przeprowadzania obowiązkowej oceny ryzyka, postulujemy przeprowadzenie konsultacji z podmiotami branżowymi

w celu wypracowania założeń analizy ryzyka zrozumiałych dla rynku i dających się realnie wprowadzić w życie. Powinny one zmierzać do wypracowania praktycznego i szczegółowego formularza lub wzoru analizy ryzyka określającego wymagania jakie musi zawierać ten dokument.

B. Uwagi szczegółowe

1. Art. 10 ust.1:

Zaproponowany przez ustawodawcę termin na odniesienie się do powiadomienia Prezesa UKE jest rażąco krótki. W sytuacji otrzymania powiadomienia w piątek abonent domeny nie dysponowałby nawet jednym dniem roboczym na ustosunkowanie się do jej treści. Proponujemy wydłużenie tego terminu do 3 dni roboczych. Taka długość terminu nie wpłynie negatywnie na realizację celów ustawy, przy jednoczesnym urealnieniu możliwości podjęcia działań przez abonenta.

2. Art. 13 ust. 5, art. 12:

Niezależnie od proponowanej zmiany modelu postępowania przed prezesem UKE, procedura rozpatrywania sprzeciwu przez prezesa UKE powinna przewidywać prawo do odwołania się od nieuwzględnienia sprzeciwu do sądu powszechnego. Ze względu na specyfikę przedmiotu oceny kognicja sądu odwoławczego – podobnie do aktualnie obowiązującego systemu odwołań od decyzji Prezesa KRRiT lub Prezesa UKE w sprawach z zakresu regulacji komunikacji elektronicznej i poczty – powinna obejmować całość okoliczności sprawy, w tym ocenę samego materiału, któremu postawiono zarzut zawierania treści pornograficznych. Odwołanie w ramach procedury sądowo-administracyjnej, z mocy prawa ograniczone tylko do kwestii legalności decyzji Prezesa UKE, nie spełnia tych wymogów. Postulujemy także takie ukształtowanie procedury odwoławczej, która umożliwi kontrolę sądową zasadności działania prezesa UKE już na etapie zgłoszenia domeny do rejestru, a nie dopiero po dokonaniu wpisu w rejestrze.

3. Art. 21 pkt 1 lit. a:

W przypadku podjęcia przez projektodawcę decyzji o zachowaniu w projekcie przepisów dotyczących treści szkodliwych oraz obowiązku przeprowadzenia oceny ryzyka w przypadku niewypełnienia lub nienależytego wypełnienia tego obowiązku postulujemy wprowadzenie mechanizmu wezwania dostawcy usługi do zaniechania naruszeń poprzedzającego nałożenie kary pieniężnej. Naruszenie tego obowiązku, z uwagi na brak skorelowanych z nim dodatkowych działań, wykazuje znikomą szkodliwość społeczną, a co za tym idzie, natychmiastowe nakładanie kar pieniężnych w przypadku jego naruszenia jest nieproporcjonalne.

4. Art. 21 pkt 1 lit. b:

Obecne brzmienie przepisu przewiduje możliwość nałożenia kary na pieniężnej na usługodawcę, który nie wypełnia obowiązku stosowania weryfikacji wieku w przypadku, gdy na stronie internetowej usługodawcy dostępne są treści szkodliwe. Jest to sprzeczne z założeniem art. 4 ust.1, który nakłada obowiązek weryfikacji wieku na usługodawcę oferującego dostęp do treści pornograficznych, a nie szkodliwych.

5. Uzasadnienie do art. 2

Zwracamy uwagę, że wykluczenie ze skutecznych metod weryfikacji wieku kart debetowych nie jest słuszne i nie przystaje do realiów polskiego rynku płatniczego. Karty debetowe stanowią znaczną większość kart płatniczych wykorzystywanych w Polsce. Ograniczenie możliwości weryfikacji wieku jedynie do kart kredytowych niesłusznie pozbawiłoby wielu użytkowników wygodnej i skutecznej metody uwierzytelnienia i potwierdzenia pełnoletności w Internecie.

Na podstawie identyfikatorów kart debetowych organizacje płatnicze są w stanie skutecznie zweryfikować czy jej posiadacz jest pełnoletni i umożliwić mu bezpieczne uwierzytelnienie się w sieci. Rekomendacje brytyjskiego regulatora Ofcom, do których odnosi się Ministerstwo, są w tym zakresie nieprecyzyjne i niesłusznie wskazują, że skuteczną weryfikację gwarantują jedynie karty kredytowe, które są dostępne tylko dla osób pełnoletnich. Wg danych NBP, na koniec września 2024 r. na krajowym rynku wydanych było 45,9 mln kart płatniczych, w tym tylko 5 mln kart kredytowych.

Co ważne, weryfikacja pełnoletności i uwierzytelnienie za pomocą kart płatniczych nie wymagają ujawniania tożsamości posiadacza karty i gwarantują odpowiednią ochronę danych osobowych. Organizacje płatnicze są w stanie przekazać wydzieloną informację o pełnoletności posiadacza karty bez ujawniania dodatkowych danych, analogicznie do funkcjonalności planowanej w EU Digital Identity Wallet.

Zdajemy sobie sprawę, że zgodnie z koncepcją projektodawcy wiążące warunki weryfikacji wieku mają wynikać z ogólnej definicji zapisanej w ustawie. W związku z tym, nie proponujemy wpisania kart debetowych i kredytowych wprost do ustawy, ale zdecydowanie sugerujemy uznanie ich za skuteczne metody weryfikacji pełnoletności w zaleceniach, które wyda Minister Cyfryzacji. W przypadku ewentualnego wydania zaleceń w formie wiążącego rozporządzenia, jak proponuje obywatelski projekt dot. weryfikacji wieku procedowany w Sejmie, także będziemy proponować uwzględnienie w nim kart debetowych i kredytowych jako skutecznych narzędzi uwierzytelnienia i weryfikacji pełnoletności w Internecie.

Jednocześnie, z uznaniem zauważamy, że projektodawca dostrzega możliwość wykorzystania potencjału narzędzi płatniczych, otwartej bankowości i portfeli cyfrowych jako skutecznych metod weryfikacji wieku oraz bierze pod uwagę istniejące rekomendacje, które wskazują na ich skuteczność. Doceniamy w szczególności, że obok rozwiązań płatniczych, Ministerstwo zwraca szczególną uwagę na potencjał wykorzystania EU Digital Identity Wallet.

Dziękując za możliwość wzięcia udziału w konsultacjach i przekazania stanowiska AmCham, deklarujemy dalszą gotowość do udziału w procesie legislacyjnym. W razie jakichkolwiek pytań, pozostajemy do dyspozycji.

Z wyrazami szacunku

Marta Pawlak, dyrektorka ds. prawnych i polityk publicznych