Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji
Sekcja AI Poland

Warszawa, dn. 03.07.2026 r.
KIGEiT/1173/07/2026

Komisja Europejska
Rue de la Loi 200
1049 Bruksela

STANOWISKO SEKCJI AI POLAND KIGEIT
w sprawie projektu rozporządzenia Parlamentu europejskiego i Rady
CLOUD AND AI DEVELOPMENT ACT (CADA)

Sekcja AI Poland KIGEIT (SAIPL KIGEiT)[1] popiera cele CADA w zakresie wzmocnienia europejskiej suwerenności technologicznej, lecz ocenia, że projekt w obecnej formie nie osiągnie tych celów bez istotnych poprawek. Kluczowe słabości to: brak prawnie wiążącej definicji suwerennej chmury, dobrowolność mechanizmów zamówień publicznych, nieefektywna walka z sovereignty washing oraz zbyt słabe przepisy o oprogramowaniu open source.

Niniejsze stanowisko zawiera sześć priorytetowych rekomendacji, których wdrożenie SAIPL KIGEIT uznaje za warunek konieczny realnego wzmocnienia pozycji europejskich podmiotów sektora chmury i AI w Europie i realizację wniosków z raportu Draghiego.

1. WPROWADZENIE DO CADA

Projekt rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego ramy środków wzmacniających europejski ekosystem chmury i AI (Cloud and AI Development Act, CADA), opublikowany przez Komisję Europejską w dniu 3 czerwca 2026 r. (COM(2026) 502 fina[2]l), stanowi ważny akt prawny regulujący europejski rynek technologii cyfrowych w zakresie chmury obliczeniowej i AI. CADA jest częścią Pakietu Suwerenności Technologicznej i wpisuje się w priorytety określone w raporcie Draghiego o przyszłości europejskiej konkurencyjności, Planie Działania AI Continent oraz strategii Apply AI.

Główne cele rozporządzenia obejmują:

- potrojenie zdolności obliczeniowych UE do 2030 r. poprzez usunięcie barier dla budowy centrów danych,
- ustanowienie zharmonizowanego unijnego ram suwerenności chmurowej (Union assurance levels 1–4),
- wsparcie europejskich dostawców usług chmurowych i AI w konkurowaniu z dominującymi hiperscalerami spoza UE,
- promocję rozwiązań open source jako instrumentu suwerenności technologicznej.

Zrzeszone w ramach SAIPL podmioty uważają, że CADA, mimo wartościowych założeń, w obecnym kształcie nie zapewni rzeczywistej suwerenności chmurowej Europy. Przepisy dotyczące zamówień publicznych pozostają dobrowolne dla państw członkowskich, brakuje wiążącej definicji suwerennej chmury, a mechanizmy przeciw udawaniu suwerennej chmury (tzw. sovereign washing) są niewystarczające. Bez istotnych poprawek rozporządzenie utrwali zależność od podmiotów spoza UE, zamiast ją eliminować.

2. OCENA OGÓLNA CADA

2.1 Elementy pozytywne

SIAPL KIGEIT docenia następujące elementy projektu:

- wprowadzenie czterostopniowych ram suwerenności (Union assurance levels 1-4) jako zharmonizowanego narzędzia oceny wiarygodności dostawców chmurowych co stanowi dobry krok w kierunku przejrzystości rynku;
- ustanowienie mechanizmu strategicznych projektów centrów danych (data centre strategic projects) z możliwością przyspieszenia procedur administracyjnych i wsparcia inwestycyjnego;

[1] https://kigeit.org.pl/sekcja-ai-poland-kigeit-saipl/

[2] https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada

- powołanie EuroCloud Federation jako platformy wymiany zasobów chmurowych między podmiotami sektora publicznego państw członkowskich;
- uwzględnienie aspektów łańcucha dostaw oprogramowania (SBOM, kontrola kodu źródłowego) w kryteriach audytu dla poziomów 2-4;
- ustanowienie mechanizmu wspólnych zamówień publicznych (joint procurement) jako instrumentu konsolidacji popytu sektora publicznego;

2.2 Elementy negatywne – do poprawy

Jednocześnie SAIPL KIGEIT identyfikuje następujące zasadnicze słabości, wymagające pilnej korekty na etapie procesu legislacyjnego:

2.2.1 Brak wiążącej definicji tzw. suwerennej chmury

CADA nie zawiera prawnie egzekwowalnej definicji "suwerennej chmury" ani "suwerennego dostawcy chmury". Czterostopniowe ramy Union assurance levels opisują techniczne i operacyjne kryteria, lecz nie tworzą kategorii prawnej, która mogłaby stanowić podstawę preferencji zakupowych, wsparcia publicznego lub priorytetyzacji w zamówieniach. Brak takiej definicji otwiera drzwi do sovereignty washing – zjawiska, w którym podmiot spoza UE, spełniając jedynie minimalne wymogi formalne (np. rejestracja europejskiej spółki zależnej, umieszczenie serwerów w UE), uzyskuje dostęp do wszystkich benefitów przewidzianych dla europejskich podmiotów.

2.2.2 Dobrowolność mechanizmów zamówień publicznych

Artykuł 32 CADA obliguje instytucje zamawiające do stosowania "kryteriów unijnej wartości dodanej" w zamówieniach usług chmurowych, lecz nie ustanawia żadnych wiążących progów, wartości docelowych ani wymogów udziału europejskich dostawców. Sprawozdawczość dla państw członkowskich (art. 33) jest mechanizmem monitorowania, nie wykonania. Wobec dominacji trzech hiperscalerów (kontrolujących ok. 70% rynku UE) i braku wiążących preferencji europejskich, naturalny efekt inercji zakupowej administracji publicznej będzie utrwalał status quo.

2.2.3 Nieefektywny mechanizm samocertyfikacji poziomu 1

Poziom 1 (Union assurance level 1) opiera się wyłącznie na samocertyfikacji dostawcy. Przy braku obowiązku zewnętrznego audytu stanowi de facto pusty certyfikat, który może być nadużywany przez podmioty niespełniające materialnych kryteriów suwerenności. Jednocześnie to właśnie poziom 1 będzie najczęściej stosowany w zamówieniach publicznych sektora o niskim ryzyku.

2.2.4 Osłabione przepisy o open source

Artykuł 41 CADA ogranicza zasadę "open source first" do obowiązku zachęcania organów publicznych do stosowania rozwiązań open source bez żadnej sposobu egzekwowania mocniejszego stawiania na open source. Artykuł 42-43 dotyczący zasady "public money, public code" nakłada wyłącznie obowiązki katalogowe i tylko gdy organ publiczny sam posiada prawa własności intelektualnej. Brak obowiązku udostępniania oprogramowania wytworzonego ze środków publicznych w ramach licencji open source (gdy prawa posiada wykonawca) stanowi utracony impuls dla budowy europejskiego ekosystemu open source.

2.2.5 Ryzyko nadużycia derogacji dla krajów trzecich (art. 18)

Możliwość uznania przez KE niektórych państw trzecich za równoważne (ekwiwalentne) pod względem suwerenności i tym samym dopuszczenie kontrolowanych przez nie podmiotów do poziomu 3 niesie poważne ryzyko. Procedura decyzji implementacyjnej Komisji musi być obwarowana rygorystycznymi kryteriami i podlegać regularnym przeglądom, a nie stanowić instrumentu dyplomatycznego nacisku.

3. ZAGROŻENIE UDAWANIEM SUWERENNOŚCI (TZW. SOVEREIGNTY WASHING)

Sovereignty washing to praktyka pozornego spełniania kryteriów suwerenności przy faktycznym utrzymaniu zależności strukturalnych od podmiotów i prawa spoza UE. To najważniejsze wyzwanie regulacyjne w Europie w zakresie chmury, na które obecne przepisy CADA skutecznie nie odpowiadają.

SAIPL KIGEIT identyfikuje następujące typowe scenariusze:

Scenariusz sovereignty washing	Mechanizm przeciwdziałania - propozycja SAIPL KIGEIT
Serwery w Europie, klucze kryptograficzne wydane europejskiej spółce zależnej, ale R&D i zarząd poza UE	Kryterium rzeczywistego centrum decyzyjnego: zarząd, R&D i cykl życia produktu muszą znajdować się w EU/EEA/EFTA i być weryfikowane przez rejestry podatkowe i listy płac

Scenariusz sovereignty washing	Mechanizm przeciwdziałania - propozycja SAIPL KIGEIT
Joint venture z europejską firmą - podmiot formalnie europejski, ale technologia, własność intelektualna pozostaje poza UE	Przejrzystość łańcucha własności do poziomu UBO (≤15% próg wprowadzony w ramach VI dyrektywy AML); zakaz ukrytej kontroli przez umowy licencyjne lub joint venture
Pracownicy UE posiadający dostęp administracyjny, ale fizycznie pozostający pod nadzorem struktur spoza UE	Audyt ścieżek dostępu uprzywilejowanego (PAM); wymóg, by personel operacyjny był obywatelami UE rezydującymi w UE na poziomach 3-4
Samocertyfikacja poziomu 1 bez niezależnej weryfikacji	Obowiązkowy audyt zewnętrzny od poziomu 1 dla firm o przychodach na terenie EU powyżej 100 mln EUR; lista akredytowanych audytorów prowadzona przez ENISA; zakaz konfliktu interesów
Dane klientów pozostają w UE, ale telemetria i metadane eksportowane są do zagranicznego centrum danych	Eksplicytne objęcie telemetrii, metadanych i logów operacyjnych klauzulą o lokalizacji danych; weryfikacja przez diagramy przepływu danych

Skuteczne przeciwdziałanie sovereignty washing wymaga przejścia od podejścia opartego na formalnych przesłankach (rejestracja, lokalizacja infrastruktury) do podejścia opartego na kontroli faktycznej (Effective Control Test), obejmującego zarówno prawne, jak i techniczne oraz ekonomiczne aspekty zależności czy własności intelektualnej. Zachowanie hyperscalers zakładających spółki JV, wskazuje, że bez zmian podejścia w przepisach, nie zostaną zrealizowane rekomendacje przewidziane w raporcie Draghiego w zakresie zwiększenia udziałów europejskich podmiotów chmurowych.

4. OCENA UNION ASSURANCE LEVELS - PROPOZYCJE WZMOCNIENIA

Aneks II do projektu CADA ustanawia kryteria dla czterech poziomów Union assurance. Poniżej SAIPL KIGEIT przedstawia ocenę obecnych kryteriów wraz z propozycjami wzmocnienia:

Poz.	Nazwa	Tryb oceny	Kluczowe kryteria	Docelowe zastosowanie
1	Podstawowy	Samocertyfikacja – do zmiany na obowiązkowy dla spółke 100 mln EUR	Infrastruktura w UE, dane klientów w UE, dostawca zarejestrowany w UE, obowiązkowy audyt dla firm powyżej 100 mln EUR obrotu na terenie EU	Zamówienia publiczne o niskim ryzyku
2	Podwyższony	Audyt niezależny	j.w. + personel w UE (opcjonalnie obywatele UE), brak wsparcia technicznego spoza UE, SBOM, własność intelektualna, B+R na terenie EU	Większość usług publicznych
3	Wysoki	Audyt + weryfikacja KE	j.w. + personel wyłącznie obywatele UE, brak kontroli spoza UE (lub derogacja KE), separacja z podmiotami zagranicznymi	Infrastruktura krytyczna, obrona
4	Najwyższy	Audyt + certyfikat EUCS High	j.w. + pełna kontrola software supply chain, brak jakiejkolwiek kontroli podmiotów trzecich	Dane niejawne, bezpieczeństwo narodowe

4.1. Kluczowe luki w kryteriach

- Kryterium (g) Aneksu II dotyczące braku praw krajów trzecich do raportowania luk w zabezpieczeniach jest jedynym mechanizmem anty-sovereignty washing na tym poziomie. SAIPL KIGEIT postuluje wprowadzenie obowiązkowej deklaracji własności rzeczywistej (UBO), weryfikowanej przez rejestr BRIS. Poziom 1 (samocertyfikacja zmieniony na audyt dla spółek 100 mln EUR):
- Kryterium (i)(ii) dotyczące oprogramowania podmiotów z krajów trzecich wymaga, by dostawca wykazał "udokumentowany plan migracji" w przypadku awarii dostawcy lub ograniczeń kraju trzeciego. SAIPL KIGEIT postuluje, by plan migracji był wymagany ex ante i testowany w rzeczywistych ćwiczeniach (disaster recovery drills), nie tylko deklarowany. Poziom 2–3 (audyt zewnętrzny):
- Kryterium (i)(ii) dotyczące "zachowania skutecznej kontroli" nad komponentami oprogramowania jest sformułowane zbyt ogólnie. SAIPL KIGEIT postuluje doprecyzowanie, że żaden podmiot z kraju trzeciego nie może posiadać >15% praw głosu w organach decyzyjnych dostawcy komponentu ani prawa veta w sprawach dotyczących bezpieczeństwa. Poziom 2-4 (najwyższy):

5. ZAMÓWIENIA PUBLICZNE JAKO NARZĘDZIE POLITYKI PRZEMYSŁOWEJ

SIAPL KIGEIT podziela stanowisko, że zamówienia publiczne, odpowiadające za ok. 15% PKB UE, stanowią skuteczny instrument kształtowania rynku usług chmurowych po stronie popytu. Niestety CADA w obecnym kształcie nie korzysta z tego potencjału.

5.1. Status quo i jego skutki

Artykuł 30 CADA nakłada na instytucje zamawiające obowiązek zakupu usług co najmniej na poziomie 1, a w przypadku usług istotnych dla porządku publicznego - na poziomie 2, 3 lub 4. Artykuł 32 wymaga stosowania kryteriów unijnej wartości dodanej. Jednak:

- brak wiążącego udziału procentowego europejskich dostawców oznacza, że kryteria unijnej wartości dodanej mogą być stosowane jako czynnik poboczny, a nie determinujący wybór oferty.
- brak mechanizmu preferencji europejskiej własności intelektualnej (European Preference) – wzorowanego na BABA (Stany Zjednoczone) czy indyjskiej preferencji krajowej - oznacza, że przy równoważności funkcjonalnej ofert europejskich i pozaeuropejskich brak obligatoryjnego rozstrzygnięcia na korzyść europejskiej.
- System sprawozdawczości (art. 33) generuje dane, ale nie tworzy mechanizmów egzekucji celów.

5.2. Rekomendacje SAIPL KIGEIT dla wzmocnienia przepisów zamówień publicznych

- CADA lub rewidowane Dyrektywy zamówieniowe powinny ustanowić wiążący cel, zgodnie z którym co najmniej 50% wydatków administracji publicznej na usługi chmurowe do 2030 r. powinno trafiać do dostawców posiadających certyfikację Union assurance level 2 lub wyższą i spełniających definicję suwerennego dostawcy europejskiego z UBO<15%. Zalecenie: wiążący KPI zamówień
- Dla zamówień powyżej progu unijnego i dotyczących infrastruktury krytycznej powinna istnieć formalne domniemanie na rzecz wybrania oferty europejskiego suwerennego dostawcy, gdy istnieje funkcjonalny odpowiednik rozwiązania spoza UE. Wybór dostawcy spoza UE powinien wymagać pisemnego uzasadnienia i być publicznie dostępny. Zlecenie: Domniemanie na rzecz rozwiązań europejskich
- Dla zamówień powyżej progu unijnego podział na części powinien być obowiązkowy (a nie jedynie zalecany), aby ułatwić udział MŚP i zapobiec monopolizacji całych kontraktów przez jednego hiperscalera. Zalecenie: obowiązkowy podział na części
- Katalog dostawców suwerennych (Tech Sovereignty Catalogue) powinien być prowadzony przez ENISA i stanowić referencję dla instytucji zamawiających; wpis do katalogu powinien być warunkiem ubiegania się o zamówienia powyżej progu unijnego dla określonych kategorii usług. Zalecenie: Tech Sovereignty Catalogue jako instrument
- Dostawcy korzystający z preferencji europejskiej mogliby dodatkowo demonstrować aktywny udział w uznanej federacji europejskiej (np. IPCEI-CIS, SIMPL, SECA) i spełniać wymogi interoperacyjności określone przez KE. Zalecenie: Federacja i interoperacyjność jako warunek dostępu do preferencji

6. SZEŚĆ PRIORYTETOWYCH REKOMENDACJI

Na podstawie powyższej analizy formułujemy następujące rekomendacje legislacyjne na etap negocjacji w Parlamencie Europejskim i Radzie:

Rekomendacja 1: prawnie wiążąca definicja suwerennej chmury

CADA musi zawierać w art. 2 lub w odrębnym artykule definicji jasną, egzekwowalną definicję "suwerennej chmury" i "suwerennego europejskiego dostawcy chmury" obejmującą:

- Kontrolę prawną: siedziba i centralna administracja w UE/EEA/EFTA; europejska większość własności i praw głosu (weryfikacja UBO); brak jurysdykcyjnej ekspozycji na prawa extraterytorialne (U.S. CLOUD Act, FISA).
- Kontrolę operacyjną: cała infrastruktura (datacenter, DR, backup) w UE; większość działalności R&D w EU/EEA/EFTA; skuteczna kontrola łańcucha dostaw dla komponentów krytycznych.
- Zakaz sovereignty washing: definicja powinna wyraźnie wykluczać podmioty kontrolowane przez entity spoza UE przez joint venture lub umowy licencyjne, nawet jeśli formalnie zarejestrowane w UE.

Rekomendacja 2: wiążące cele zamówień publicznych

Art. 32 lub 33 CADA powinny zostać uzupełnione o wiążące cele ilościowe:

- Co najmniej 50% wydatków publicznych na usługi chmurowe do 2030 r. powinno trafiać do suwerennych europejskich dostawców (Union assurance level 2+).
- Coroczne raportowanie realizacji celów przez państwa członkowskie z możliwością zastosowania mechanizmu zaleceniowego KE w przypadku niedostatecznych postępów.
- Domniemanie na rzecz europejskich rozwiązań dla zamówień powyżej progu unijnego dotyczących infrastruktury krytycznej, z obowiązkiem uzasadnienia pisemnego przy wyborze dostawcy spoza UE.

Rekomendacja 3: wzmocnienie mechanizmów anty-sovereignty washing

Aneks II (kryteria audytu) powinien zostać uzupełniony o:

- Wymóg przejrzystości rzeczywistej własności (UBO) już od poziomu 1, weryfikacja przez BRIS i rejestr UBO zgodnie z dyrektywą 6AMLD.
- Zakaz liczenia jako europejskiego podmiotu, w którym podmiot spoza EU/EEA/EFTA sprawuje kontrolę faktyczną przez umowy licencyjne, długoterminowe umowy zaopatrzeniowe lub depozyty kodu źródłowego.
- Obowiązkowy test efektywnej kontroli obejmujący: strukturę własności, prawa głosu, skład zarządu, zależności technologiczne i finansowe.
- Audyt obowiązkowy od poziomu 1 w przypadku podmiotów z rocznymi przychodami ponad 100 mln EUR na terenie UE
- Od poziomu 2 posiadanie własności intelektualnej, B+R na terenie EU – ale nie na zasadzie licencji czy oddziałów
- Obowiązek zgłoszenia do organu krajowego każdego wniosku zewnętrznego o dostęp do danych klientów lub zakłócenie usługi (w ciągu 24h).

Rekomendacja 4: wzmocnienie przepisów o oprogramowaniu open source

Art. 41-42 CADA powinny zostać wzmocnione:

- "Open source first" powinno być wyrażone jako domniemanie prawne, od którego odejście wymaga udokumentowanego uzasadnienia (odwrócenie ciężaru dowodu), nie jedynie "zachęty".
- Zasada "public money, public code" powinna nakładać obowiązek udostępnienia kodu źródłowego oprogramowania wytworzonego ze środków publicznych na licencji open source, niezależnie od tego, kto posiada prawa IP (z możliwością wyłączenia dla oprogramowania wrażliwego dla bezpieczeństwa narodowego).
- Organy publiczne powinny być zobowiązane do prowadzenia SBOM (Software Bill of Materials) dla całego używanego oprogramowania od 2028 r.
- Katalog Rozwiązań Open Source (art. 43) powinien dawać preferencje w zamówieniach publicznych.

Rekomendacja 5: federacja europejskich dostawców chmury jako cel przemysłowy

CADA powinien ustanowić europejską federację jako cel przemysłowy z operacyjnymi mechanizmami wdrożenia:

- Wykorzystanie obowiązkowego publicznego standardu oferującego interoperacyjność dla dostawców ubiegających się o preferencje w zamówieniach publicznych.
- Konwergencja istniejących inicjatyw (IPCEI-CIS, SIMPL, SECA, Tech Sovereignty Catalogue) pod mandatem koordynacyjnym KE, z jasnym harmonogramem do 2028 r.
- Dostęp do zamówień powyżej progu UE uwarunkowany przynależnością do uznanej federacji i spełnianiem standardu interoperacyjności.
- Miks finansowania (EIB + środki publiczne) dla dostawców MŚP uczestniczących w federacji w regionach niedoboru zdolności obliczeniowych.

Rekomendacja 6: procedury lokalizacyjne centrów danych i dostęp do energii

Przepisy Tytułu III (datacenter acceleration zones) wymagają wzmocnienia:

- Wiążące terminy dla organów krajowych: decyzja o lokalizacji centrum danych w specjalnej strefie akceleracyjnej w ciągu 12 miesięcy (zamiast orientacyjnych); dla projektów strategicznych - 6 miesięcy
- Obowiązek wskazania przez operatorów sieci elektroenergetycznych dostępnych mocy przyłączeniowych w ciągu 6 miesięcy od wniosku – celem eliminacja bariery kolejki przyłączeniowej.

- Priorytet w dostępie do odnawialnych źródeł energii dla centrum danych posiadającego certyfikację Union assurance level 2+, spełniającego wymogi PUE ≤ 1.2.
- Miks finansowania: Europejski Bank Inwestycyjny powinien mieć mandat do finansowania centrów danych europejskich suwerennych dostawców na preferencyjnych warunkach (gwarancja dla 30% CAPEX).

SAIPL KIGEIT ocenia, że Cloud and AI Development Act stanowi historyczną szansę na realną przebudowę europejskiego rynku usług chmurowych w kierunku suwerenności i konkurencyjności. Jednak szansa ta może zostać zmarnowana, jeżeli w toku procesu legislacyjnego nie zostaną wprowadzone opisane powyżej zmiany.

SAIPL KIGEIT pragnie podkreślić, że: suwerenność chmurowa Europy wymaga nie tylko infrastruktury na terenie UE, ale przede wszystkim rzeczywistej kontroli prawnej, technologicznej i ekonomicznej sprawowanej przez europejskie podmioty. Bez wiążących definicji, egzekwowalnych celów zamówień publicznych i skutecznych mechanizmów anty-sovereignty washing CADA stanie się kolejnym dokumentem deklaratywnym, który nie zmieni struktury rynku zdominowanego przez trzech zewnętrznych hiperscalerów.

SAIPL KIGEIT deklaruje gotowość do aktywnego udziału w procesie legislacyjnym, zarówno na poziomie krajowym, jak i europejskim, oraz do współpracy z innymi organizacjami branżowymi (DIGITAL SME Alliance, Digital Europe) czy inicjatyw oddolnych jak EuroStack na rzecz wypracowania stanowisk wzmacniających europejską suwerenność technologiczną.

Stefan Kamiński
Prezes Zarządu KIGEiT

Piotr Mieczkowski
Przewodniczący Zarządu Sekcji SAIPL

Signature Not Verified
Dokument podpisany przez Stefan Kamiński
Data: 2026.07.03 09:49:19 CEST
Powód: Złożenie podpisu