Stanowisko Polskiej Izby Informatyki i Telekomunikacji (PIIT)
wobec projektu aktu UE w sprawie rozwoju chmury obliczeniowej
i sztucznej inteligencji (CADA)

1. Kontekst

Cel nadrzędny projektu to zapewnienie UE mocy obliczeniowej adekwatnej do potrzeb oraz ograniczenie zależności od dostawców chmury i AI spoza Europy, poprzez promowanie B+R, przyspieszenie budowy centrów danych, zapewnienie dostępności suwerennej chmury i AI oraz wsparcie wdrożeń w sektorze publicznym.

2. Stanowiska tematyczne

2.1. Podstawa prawna i forma aktu

PIIT kwestionuje art. 114 TFUE jako podstawę prawną. Przepis art. 114 TFUE nie daje ogólnej kompetencji do regulowania rynku wewnętrznego. Środek ciężkości aktu leży poza harmonizacją rynku. Konkretne przepisy dotyczą zmiana w prawie zamówień publicznych oraz powołania nowych form organizacyjno-prawnych dla współpracy, obok istniejących. Właściwą podstawą prawną pozostają art. 53 ust. 1, art. 62 oraz dodatkowo art. 114 tfue. Do katalogu celów wystarczyłby komunikat, wnioski Rady lub najwyżej dyrektywa. Postulujemy nowelizację dyrektywy o zamówieniach zamiast nowego rozporządzenia.

2.2. Dostawcy spoza UE i „zaufani partnerzy"

PIIT popiera podniesienie poziomu bezpieczeństwa systemów IT używanych w sektorze publicznym, jak również wyeliminowanie nieuczciwej konkurencji w postaci niedozwolonej pomocy publicznej. Ze zrozumieniem odnosi się do ograniczenia, a nawet wyeliminowania ryzyka korzystania przez państwa spoza Unii z ekstraterytorialnych narzędzi prawnych i technicznych do sięgania po dane sektora publicznego, bez jego wyraźnej zgody. Izba popiera suwerenność cyfrową, która odpowiada powyższym celom, ale nie eliminuje technologicznych partnerów tylko na podstawie kryterium geograficznego. Zbyt radykalne stanowisko grozi odizolowaniem UE od innowacji i zakłóceniem globalnych łańcuchów dostaw, dotykającym również europejskich dostawców.

2.3. Poziomy zapewnienia suwerenności (UAL, „level of assurance")

PIIT uważa sam termin „level of assurance" za nieprecyzyjny i mylący; proponuje zrozumiałe pojęcie (np. unijny certyfikat suwerenności, poświadczenie zgodności z wymogami suwerenności). Lista wymogów na poszczególnych poziomach powinna być przedmiotem pogłębionej analizy. W obecnym kształcie nie może być zaakceptowana. Gdy ocena ryzyka (art. 29) wskaże, że działalność zamawiającego ma znaczenie dla porządku publicznego — w sektorach z załączników I/II dyrektywy NIS2 oraz w obszarach bezpieczeństwa narodowego, wewnętrznego, granic, obrony, wymiaru sprawiedliwości i ścigania to w tak szeroko zdefiniowanych branżach będzie można kupować „only…

cloud computing services that have been recognised as having a Union assurance level 2, 3 or 4". Odstępstwa (art. 30 ust. 4) są wąskie: brak uznanej usługi i brak alternatywy, wcześniejszy przetarg bez ofert, albo nieproporcjonalny koszt. Wymogi suwerenności, ujęte w załączniku II, są niezwykle rozbudowane. Natomiast lista wymogów powinna być definiowana wąsko. Lista ta będzie wymagać szczegółowych konsultacji, zwłaszcza, że niektóre przepisy mogą wywoływać niespodziewane skutki.

Nawet na najniższym poziomie UAL 1 propozycje uniemożliwią realizację kluczowych funkcji z zakresu cyberbezpieczeństwa w skali globalnej, ze względu na wymóg przechowywania wszystkich danych telemetrycznych, w tym wzorców cyberzagrożeń, w Europie. PIIT sugeruje rozważenie usunięcia wymogów lokalizacji danych w odniesieniu do metadanych i danych telemetrycznych na poziomach UAL 1 i 2 (Załącznik II, sekcje 1.1c i 2.1c). Analogicznie celowe byłoby przeanalizowanie połączenia poziomów UAL 3 i 4 w jeden poziom, który umożliwi zaufanym operatorom spoza UE odgrywanie roli wspierającej w odniesieniu do ściśle niezależnych, obsługiwanych przez podmioty europejskie rozwiązań suwerennych, w tym poprzez dostarczanie bazowego oprogramowania. Izby uważa, że warto rozważyć odwrócenie przysługującego Komisji uprawnienia do ustanawiania odstępstw (Załącznik II, sekcja 3(g)). Godzi ono w zaufanych partnerów Unii. Komisja mogłaby cofać dopuszczenie w drodze uzasadnionej decyzji.

Uprawnieniu Komisji do uchylania decyzji państw członkowskich w ramach oceny ryzyka suwerenności (art. 29 ust. 5) może skutkować ryzykiem naruszenia art. 4 TUE i ingerencji w bezpieczeństwo narodowe.

2.4. Proporcjonalność wymogów UAL dla MŚP

Projekt przewiduje na poziomie UAL 1 samoocenę z unijnym oświadczeniem o zgodności, automatycznie uznawanym w przypadku MŚP we wszystkich państwach członkowskich oraz cel co najmniej 25% zamówień chmurowych i AI dla innowacyjnych MŚP. PIIT ocenia te rozwiązania pozytywnie. Problem pojawia się na poziomie UAL 2, gdzie wymagany jest niezależny audyt prowadzony na koszt dostawcy. Koszt takiego audytu jest w przeważającej mierze stały i nie rośnie wraz z przychodem: dla globalnego dostawcy to pozycja w budżecie, dla firmy zatrudniającej kilka osób — bariera zamykająca dostęp do segmentu zamówień o podwyższonej wrażliwości. Skoro znaczna część działalności sektora publicznego zostanie przypisana do UAL 2, cel 25% udziału MŚP pozostanie deklaracją bez pokrycia w rzeczywistej dostępności certyfikacji.

PIIT postuluje audyt uproszczony, o ograniczonym zakresie, na poziomie UAL 2 dla podmiotów spełniających definicję MŚP z zalecenia 2003/361/WE, z pełnym reżimem audytowym od poziomu UAL 3.

2.5. Kumulatywne kryteria zgodności i ocena punktowa na poziomach UAL 2–4

Załącznik II przewiduje kumulatywne kryteria dla każdego poziomu, a audyt na poziomach UAL 2–4 kończy się zasadniczo wynikiem pozytywnym albo negatywnym. Taka konstrukcja premiuje podmioty zdolne nabyć zgodność w całości i jednorazowo, a wyklucza dochodzenie do niej etapami. PIIT postuluje dopuszczenie alternatywnych lub kompensujących środków technicznych, ocenianych pod

kątem celu danego wymagania i rzeczywiście redukowanego ryzyka — przykładowo przechowywanie kluczy szyfrujących poza infrastrukturą dostawcy ogranicza ryzyko dostępu do treści danych i mogłoby być uznane za środek kompensujący w odniesieniu do tego konkretnego ryzyka.

Ocenę punktową zgłaszają w podobnym duchu również najwięksi dostawcy spoza UE, kierując się utrzymaniem dostępu do rynku, na którym już działają; z perspektywy sektora MŚP kluczowe jest natomiast to, by podmioty budujące zgodność stopniowo, w miarę wzrostu, mogły na ten rynek w ogóle wejść. Postulat ten jest zbieżny z propozycją Izby dotyczącą systemu punktacji, zgłoszoną w pkt 2.12.

2.6. Odpowiedzialność dostawcy warstwy aplikacyjnej za infrastrukturę podwykonawcy

Definicja usługi chmurowej w projekcie obejmuje zdalny, skalowalny dostęp do zasobów obliczeniowych, w tym zdalne udostępnianie systemów sztucznej inteligencji. W konsekwencji dostawca aplikacji AI świadczonej jako usługa może sam być dostawcą usługi chmurowej w rozumieniu rozporządzenia, a globalnego operatora infrastruktury traktować jako swojego podwykonawcę. Projekt może więc uczynić dostawcę warstwy aplikacyjnej bezpośrednio odpowiedzialnym za spełnienie kryteriów dotyczących infrastruktury jego podwykonawcy, mimo że dostawca aplikacji nie ma technicznych ani kontraktowych środków pozwalających samodzielnie zapewnić lub zweryfikować tę zgodność. Przykładowo wymóg z Załącznika II sekcja 1.1(c), aby dane klienta, w tym metadane i dane telemetryczne, pozostawały wyłącznie w UE, obejmuje również podwykonawców dostawcy — dostawca warstwy aplikacyjnej nie jest w stanie samodzielnie wykazać zgodności architektury telemetrycznej globalnego operatora, na którego infrastrukturze buduje. Do tego dochodzi kaskada kontraktowa: doświadczenia z wdrażania rozporządzenia DORA i dyrektywy NIS2 wskazują, że można oczekiwać przenoszenia wymogów i ryzyka kontraktowego na dalsze ogniwa łańcucha dostaw, które nie dysponują ani zapleczem prawnym, ani wpływem na przedmiot wymogu.

PIIT postuluje, aby rozporządzenie wprost rozgraniczało odpowiedzialność za właściwości infrastruktury bazowej — lokalizację danych, telemetrię, kontrolę operacyjną, personel i strukturę podwykonawców — od odpowiedzialności podmiotów budujących usługi na tej infrastrukturze. Dostawca warstwy aplikacyjnej powinien odpowiadać za wybór podwykonawcy posiadającego uznanie na wymaganym poziomie UAL, a nie za samodzielne wykazanie właściwości jego infrastruktury. Bez takiego rozgraniczenia każdy poziom UAL wytworzy warstwę zgodności pozornej: zobowiązania, których dalsze ogniwa łańcucha nie są w stanie ani spełnić, ani zweryfikować.

2.7. Rynek dwóch prędkości i przewidywalność odstępstw

Jeżeli usługi dla sektora publicznego zostaną związane z uznanymi usługami chmurowymi o określonym poziomie UAL, a sektor prywatny zachowa dostęp do pełnej oferty globalnej, różnica w dostępnych narzędziach rozłoży się na rynku nierówno — duży dostawca utrzyma dwa równoległe środowiska technologiczne, małego na to nie stać. Przykładowo podmiot publiczny korzystający z aplikacji AI dostarczanej przez małą firmę na infrastrukturze dostawcy spoza UE może, po ocenie ryzyka i przypisaniu poziomu UAL, zmusić dostawcę do migracji na infrastrukturę o węższej ofercie,

utrzymywania dwóch wariantów produktu albo rezygnacji z rynku publicznego — chyba że zamawiający zastosuje przewidziane w rozporządzeniu odstępstwo (np. brak porównywalnej funkcjonalnie oferty lub nieproporcjonalne koszty). Odstępstwo zależne od decyzji zamawiającego nie zapewnia jednak małemu dostawcy przewidywalnego dostępu do rynku: nie da się budować produktu ani zatrudniać ludzi w oparciu o nadzieję, że zamawiający skorzysta z wyjątku.

PIIT postuluje, aby rozporządzenie jednoznacznie wymagało ustalania poziomu UAL na poziomie konkretnej działalności sektora publicznego oraz precyzyjnie wydzielonej usługi lub komponentu chmurowego — korzystanie przez jednego dostawcę z infrastruktury o różnym poziomie zapewnienia nie powinno prowadzić do objęcia całego portfolio najwyższym z mających zastosowanie poziomów. Okres przejściowy dla usług już świadczonych sektorowi publicznemu powinien być liczony od chwili rzeczywistej dostępności uznanej oferty o porównywalnej funkcjonalności, a nie od daty rozpoczęcia stosowania rozporządzenia.

2.8. Ścieżka zastępcza do przyjęcia europejskiego schematu certyfikacji (EUCS)

Poziomy UAL 2–4 odsyłają do europejskiego schematu certyfikacji cyberbezpieczeństwa usług chmurowych (EUCS), który pozostaje w przygotowaniu od 2020 r. Projekt przewiduje na okres przejściowy sekwencję zastępczą: krajowe schematy certyfikacji tam, gdzie istnieją, a w ich braku — wykazanie stosowania najwyższych standardów cyberbezpieczeństwa wynikających z prawa UE. Problemem nie jest brak ścieżki zastępczej, lecz jej kształt: fragmentacja między państwami członkowskimi, brak jednolitego standardu dowodowego oraz otwarta interpretacja pojęcia najwyższych standardów. Duży podmiot może przygotowywać się równolegle do kilku schematów krajowych i przyszłego schematu europejskiego; mała firma nie ma na to zasobów i do czasu przyjęcia schematu europejskiego nie wie, w co inwestować. PIIT postuluje, aby do czasu przyjęcia schematu europejskiego Komisja określiła w akcie wykonawczym jednolity, minimalny standard dowodowy dla ścieżki zastępczej, uznawany we wszystkich państwach członkowskich.

2.9. Przepisy przejściowe dla umów wieloletnich

Projekt nie przewiduje szczególnej ochrony umów zawartych przed rozpoczęciem jego stosowania. Roczne odroczenie stosowania rozporządzenia oraz maksymalnie dwunastomiesięczny okres migracji, gdy wymaga jej ocena ryzyka, nie rozwiązują problemu umów wieloletnich ani kosztów zmiany architektury w trakcie ich wykonywania. Praktyka rynkowa jest przewidywalna: zamawiający przeniesie nowe wymogi na wykonawcę klauzulami umownymi, a wykonawca — na podwykonawców. Mały podwykonawca w trakcie obowiązywania umowy stanie przed wyborem między kosztowną przebudową środowiska technologicznego a rozwiązaniem umowy; żadna z tych dróg nie zwiększa suwerenności, obie zwiększają ryzyko prawne po stronie najsłabszych uczestników rynku.

PIIT postuluje, aby umowy zawarte przed rozpoczęciem stosowania rozporządzenia mogły być wykonywane do końca okresu ich obowiązywania, nie krócej jednak niż przez 36 miesięcy od rozpoczęcia stosowania.

2.10. Uprawnienia Komisji i kompetencje państw członkowskich

W opinii PIIT cele i zadania ujęte w treści artykułów 3 i 4 mają charakter deklaratywny. Przewidziane w projekcie obowiązki państw członkowskich i przedsiębiorców nie przyczynią się do ich realizacji. Obowiązki są konkretne i wymagają poważnych nakładów finansowych.

Założeniem projektu jest rozbudowa i wzmocnienie systemu EDIH poprzez centralizację zarządzania nimi (art. 5 ust. 1 i 4 projektu). Jest to zaskakujące. Według sprawozdania JRC za rok 2025 w Unii działa 225 hubów / 2 355 organizacji. Zapewnia to pokrycie ~90% regionów. 151 jest finansowanych z programu „Cyfrowej Europy". Na poziomie UE działa publiczny, przejrzysty monitoring aktywności EDIH. Jednakże raport za rok 2025 zawiera przyznanie, że nie da się ocenić efektywności działania tej sieci (brak grupy kontrolnej, nie da się przypisać efektu przyczynowo), tylko 202 wiarygodne pary przed/po, dane samodeklarowane, opóźnienia w podpisywaniu umów, 44 ze 151 hubów bez zaraportowanych usług. To monitoring opisowy, cyt. „5 016 wydarzeń, 212 602 uczestników, 17 583 usług, 11 026 klientów (90% MŚP)". Podobnie analizy zlecone przez PARP dla działania FENG 2.22 pozwalają na (pozytywną) ocenę systemu i kryteriów wyboru, a nie ocenę efektywności ex post działania hubów EDIH. Zarówno na poziomie UE, jak i PARP odnotowano uwagi o znaczących obciążeniach biurokratycznych. W tej sytuacji odpowiedzią Komisji jest stworzenie kolejnych struktur zarządczych i próby ujednolicenia z Brukseli zasad działania hubów.

Izba sprzeciwia się utworzeniu Federacji EuroCloud (art. 34–36) jako jednostki organizacyjnej, pozbawionej osobowości prawnej i podlegającej wyłącznie zasadom określonym w aktach wykonawczych Komisji Europejskiej. To kolejny przejaw forsowanej przez Komisję centralizacji sektora publicznego. Dostrzega celowość współpracy jednostek sektora finansów publicznych i potencjał ich współpracy w zakresie dostępu do usług przetwarzania w chmurze, w tym korzystania z SaaS. Co do katalogu rozwiązań to w tym zakresie taka platforma w obszarze AI już istnieje. Finansowanie kolejnej z budżetu ogólnego Unii byłoby działaniem na szkodę interesów finansowych Unii. Wymyślenie podstawy prawnej do takich zachowań nie zmienia oceny takiego zachowania. Dodatkowo (motyw 73) stanowi kolejny wyłom z reżimu zamówień. Federacja mogłaby powstać jako dobrowolne zrzeszenie, w formie prawnej przewidzianej przez prawo państwa członkowskiego i tamże zarejestrowane.

2.11. Zamówienia publiczne

Na dzisiaj trudno ocenić jak odejście od znanych wszystkim procedur udzielenia zamówienia publicznego (na rzecz nie do końca określonych jeszcze zasad Komisji, art. 37–40) wpłynie na przejrzystość postępowania. Sygnalizowane korzyści to hipotetyczna możliwość obniżenia ceny dla zamawiającego, a dla oferenta znaczący lewar rynkowy pozwalający na wejście na rynki sektora publicznego w kilku państwach członkowskich jednocześnie. Dla zamawiających z p.cz. oznacza to naukę i obsługę dodatkowych procedur między Komisją a zamawiającymi. Niejasna jest relacja nowej platformy zakupowej do istniejącego portalu TED. Uwzględnienie w TED nowych wymogów polityki suwerenności (i tak obowiązkowe po ew. uchwalenie aktu) i procedur wspólnych zamówień, niekoniecznie przy udziale Komisji, wydaje się wystarczające i proporcjonalne. Możliwe jest także wspólne zamawianie przy pośrednictwie jednego z państw członkowskich i przy wykorzystaniu jego

platform zakupowych, znanych już krajowym oferentom. Forsowanie centralizacji nie zawsze jest dobrym rozwiązaniem w praktyce, choć wydaje się aksjomatem działania Komisji.

Kryterium „wartości europejskiej" (art. 32) i kryterium pochodzenia rodzą napięcie z zasadą równego traktowania i WTO GPA. Odejście od znanych procedur (art. 37–40), wspólne zamówienia i EuroCloud obniżają przejrzystość i mnożą obowiązki. Nowelizacja dyrektywy zamówieniowej to ekonomiczna ścieżka zmian na bazie znanych procedur bazowych.

Kryteria pozacenowe powinny wspierać otwarte technologie i architekturę wielochmurową (multi-cloud) przeciwdziałając uzależnieniu od jednego dostawcy.

2.12. Certyfikacja i nadzór

PIIT kwestionuje wprowadzenie odrębnego, dwustopniowego systemu certyfikacji usług, odmiennego od modelu CE i domniemania zgodności, niespójnego z AI Act. Postuluje oparcie się na istniejącym systemie certyfikacji i jednostkach notyfikowanych zamiast weryfikacji procesu i wyniku certyfikacji przez „konfederację referentów z ministerstw".

Dla oceny suwerennej kontroli nad danymi i informacjami przetwarzanymi w sektorze publicznym (dostęp podmiotów trzecich, ryzyko jurysdykcyjne, ryzyko techniczne) wskazany byłby system punktacji dopuszczającej alternatywne, skuteczniejsze środki łagodzące (np. przechowywanie kluczy szyfrujących poza chmurą).

2.13. Infrastruktura, centra danych, interoperacyjność

PIIT popiera szerokie uwzględnienie wymogów interoperacyjności, przyspieszenie przyłączeń do sieci i budowy infrastruktury (status Special Project, elastyczne umowy przyłączeniowe, PPA, strefy akceleracji, chłodzenie wodne). Opowiada się za przeciwdziałaniem uzależnieniu (uzupełnienie DMA, przenoszalność licencji, Security Equivalence).

2.14. Podsumowanie

Izba zwraca uwagę, że ryzyko systemowej zależności i koncentracji, któremu rozporządzenie ma przeciwdziałać, jest związane przede wszystkim ze strukturą rynku największych dostawców infrastruktury. Znaczna część kosztów wdrożenia może zostać przeniesiona na mniejszych dostawców aplikacji, integratorów i podwykonawców, czyli na podmioty, które nie kontrolują właściwości infrastruktury, za które mogą formalnie odpowiadać. W rezultacie regulacja może niezamierzenie zwiększyć bariery wejścia i pogłębić koncentrację, którą ma ograniczać.

3. Kluczowe postulaty

- Skoncentrowanie zmian na nowelizacji dyrektywy o zamówieniach publicznych (art. 53 ust. 1, art. 62, art. 114 TFUE), z uwzględnieniem wymogów Załącznika II.
- Oparcie certyfikacji na istniejącym systemie (CE, AI Act, NIS2) i rezygnacja z dodatkowego, równoległego reżimu.

- Analiza efektywności istniejących EDIH przed tworzeniem kolejnych struktur zarządczych.
- Stały kontakt z rynkiem na etapie prac grupy roboczej Rady, zwłaszcza przy Załączniku II, który powinien być zracjonalizowany.
- Analiza przydatności istniejących platform IT przed proponowaniem nowych; ograniczanie regulacji dla sektora IT.
- Usunięcie wymogów lokalizacji metadanych i danych telemetrycznych na UAL 1–2 (Załącznik II, sekcje 1.1c i 2.1c).
- Połączenie UAL 3 i 4 oraz odwrócenie uprawnienia do odstępstw (Załącznik II, sekcja 3(g)) — domyślne dopuszczenie zaufanych partnerów spoza UE.
- Usunięcie wymogów wobec operatorów z państw trzecich na UAL 2 (Załącznik II, sekcja 2.1(g)).
- Ograniczenie uprawnienia Komisji do uchylania decyzji państw (art. 29 ust. 5).
- Oparcie oceny suwerennej kontroli na punktacji; wsparcie interoperacyjności, przenoszalności licencji i przyspieszenia infrastruktury.
- Wprowadzenie uproszczonego audytu o ograniczonym zakresie na poziomie UAL 2 dla podmiotów spełniających definicję MŚP (zalecenie 2003/361/WE), z pełnym reżimem audytowym od poziomu UAL 3.
- Ochrona umów wieloletnich zawartych przed rozpoczęciem stosowania rozporządzenia — wykonywanie do końca okresu obowiązywania, nie krócej niż 36 miesięcy.
- Rozgraniczenie odpowiedzialności dostawcy warstwy aplikacyjnej od odpowiedzialności za właściwości infrastruktury podwykonawcy (lokalizacja danych, telemetria, kontrola operacyjna, personel, podwykonawcy).
- Ustalanie poziomu UAL na poziomie konkretnej usługi lub komponentu chmurowego, a nie całego portfolio dostawcy; liczenie okresu przejściowego od faktycznej dostępności uznanej oferty.
- Jednolity, minimalny standard dowodowy dla ścieżki zastępczej do przyjęcia europejskiego schematu certyfikacji (EUCS), uznawany we wszystkich państwach członkowskich.