CloudFerro

Stanowisko CloudFerro w sprawie projektu Cloud and AI Development Act



Europejska kontrola nad technologią warunkiem skuteczności nowych regulacji

CloudFerro popiera cele projektu Cloud and AI Development Act, w szczególności zwiększenie europejskich mocy obliczeniowych, rozwój infrastruktury chmurowej i AI oraz wzmacnianie odporności technologicznej Unii Europejskiej. Projekt rozporządzenia może stać się istotnym instrumentem europejskiej polityki przemysłowej, pod warunkiem że jego przepisy doprowadzą do rzeczywistej zmiany struktury rynku, a nie jedynie do zwiększenia liczby centrów danych zlokalizowanych w UE i wprowadzenia nowych oznaczeń zgodności.

Proponowane ramy regulacyjne będą skuteczne tylko wtedy, gdy pozwolą odróżnić infrastrukturę zlokalizowaną w Europie od technologii znajdującej się pod rzeczywistą europejską kontrolą. Sama lokalizacja infrastruktury, danych czy personelu w Unii nie zapewnia zdolności do niezależnego rozwijania, utrzymywania i świadczenia kluczowych usług. Zdolność ta zależy również od struktury właścicielskiej i kontroli operacyjnej, właściwej jurysdykcji, własności intelektualnej, dostępu do kodu źródłowego, kontroli nad aktualizacjami oraz braku krytycznych zależności od podmiotów z państw trzecich.

Europa potrzebuje dostawców zdolnych do świadczenia i rozwijania swoich usług bez konieczności uzyskiwania zgody podmiotów podlegających jurysdykcjom państw trzecich oraz bez uzależnienia od kontrolowanej przez nie technologii lub decyzji. Dlatego projekt powinien opierać się na czterech zasadach:

- europejska kontrola, a nie wyłącznie europejska lokalizacja;
- zamówienia publiczne jako narzędzie polityki przemysłowej;
- wsparcie infrastruktury i inwestycji powiązane z europejską autonomią;
- mierzenie rzeczywistych zmian struktury rynku.

Wzmacniania europejskiej kontroli nie należy traktować jako ograniczenia konkurencji. Przeciwnie, powinno ono tworzyć warunki dla bardziej konkurencyjnego, zróżnicowanego i odpornego europejskiego rynku chmury i AI.

1. Europejska kontrola, nie tylko europejska lokalizacja

1.1. Rozdzielenie poziomu zapewnienia usługi od statusu europejskiego dostawcy

Projekt rozporządzenia powinien wyraźnie rozróżniać usługę spełniającą wymogi określonego unijnego poziomu zapewnienia (Union Assurance Level) od dostawcy znajdującego się pod europejską kontrolą.

Poziom zapewnienia powinien opisywać cechy konkretnej usługi, w tym jej bezpieczeństwo, odporność, lokalizację oraz model kontroli operacyjnej. Status dostawcy kontrolowanego z Europy powinien natomiast decydować o możliwości korzystania z preferencji w zamówieniach publicznych, finansowania publicznego oraz statusu projektu strategicznego.

Nie każda bezpieczna usługa musi być świadczona przez europejskiego dostawcę. Jednocześnie nie każdy dostawca, którego usługa spełnia określone wymogi bezpieczeństwa, powinien korzystać z instrumentów europejskiej polityki przemysłowej. Instrumenty te powinny wspierać podmioty tworzące i utrzymujące w Europie rzeczywiste zdolności technologiczne, operacyjne i decyzyjne.

1.2. Test efektywnej kontroli

Uznanie dostawcy za podmiot znajdujący się pod europejską kontrolą powinno wymagać przeprowadzenia jednolitego testu efektywnej kontroli. Test powinien być stosowany zawsze, gdy podmiot ubiega się o dostęp do preferencji w zamówieniach publicznych, finansowania publicznego lub statusu projektu strategicznego.

Ocena powinna obejmować co najmniej:

- strukturę właścicielską i kontrolę korporacyjną;
- prawa głosu i veta;
- miejsce, w którym faktycznie podejmowane są decyzje;
- jurysdykcję właściwą dla dostawcy i podmiotów należących do jego grupy;
- kontrolę operacyjną nad świadczeniem usługi;
- zarządzanie dostępem uprzywilejowanym;
- własność intelektualną oraz kontrolę nad kodem źródłowym i aktualizacjami;
- zdolność do samodzielnego utrzymywania i rozwijania usługi;
- krytyczne zależności technologiczne, finansowe i kontraktowe.

Podmiot nie powinien być uznawany za dostawcę znajdującego się pod europejską kontrolą, jeżeli jego zdolność do samodzielnego świadczenia lub rozwijania usługi zależy od licencji, aktualizacji, kodu źródłowego, wsparcia lub decyzji kontrolowanych przez podmiot z państwa trzeciego. Zasada ta powinna obejmować również zależności wynikające z umów licencyjnych, joint ventures, umów wsparcia technicznego i struktur grup kapitałowych.

Taki test jest niezbędny, aby zapobiegać zjawisku sovereignty washing, w którym dostawca formalnie spełnia określone wymogi dotyczące lokalizacji lub struktury korporacyjnej, ale nadal pozostaje technologicznie lub operacyjnie zależny od podmiotu spoza Unii.

1.3. AI i cały stos technologiczny

Praktyczne wymogi dotyczące suwerenności nie powinny ograniczać się do podstawowych usług infrastruktury chmurowej. Powinny obejmować również AI-as-a-Service, platformy AI, usługi inferencji, zarządzanie modelami oraz warstwę danych. Skoro projekt obejmuje zarówno chmurę, jak i AI, wymagania odnoszące się do usług AI nie powinny być istotnie słabsze od tych dotyczących usług chmurowych.

Dostawcy powinni mieć obowiązek ujawniania krytycznych zależności technologicznych w całym stosie technologicznym. Obowiązek ten powinien obejmować w szczególności warstwy orkiestracji i zarządzania, systemy telemetrii i aktualizacji, zarządzanie tożsamością, kontrolę nad kluczami kryptograficznymi oraz inne komponenty kontrolowane przez podmioty trzecie.

Wymogi lokalizacyjne i kontrolne powinny obejmować nie tylko dane klientów, lecz również metadane, logi operacyjne, telemetrię i informacje diagnostyczne. Przekazywanie takich informacji do infrastruktury lub podmiotów kontrolowanych spoza UE może powodować zależności i ryzyka porównywalne z tymi, które dotyczą podstawowych danych klientów.

1.4. Poziom 1 jako bazowy poziom zgodności

Unijny poziom zapewnienia 1 nie powinien być utożsamiany z suwerennością ani przedstawiany jako certyfikat suwerennej chmury. Powinien być określany jako europejski bazowy poziom zgodności.

Takie rozróżnienie jest potrzebne, aby samoocena dostawcy nie była wykorzystywana do twierdzeń marketingowych sugerujących stopień kontroli lub autonomii, którego dostawca w rzeczywistości nie zapewnia.

Samooceny dostawców powinny podlegać wyrywkowym kontrolom oraz skutecznym i proporcjonalnym sankcjom za fałszywe lub wprowadzające w błąd deklaracje.

W przypadku największych dostawców oraz podmiotów kontrolowanych z państw trzecich poziom 1 powinien wymagać niezależnej weryfikacji. Skala ich działalności, dostępne zasoby oraz potencjalna ekspozycja na ryzyko uzasadniają wyższy standard niż w przypadku europejskich małych i średnich przedsiębiorstw.

1.5. Audyt i egzekwowanie wymogów

Wiarygodność systemu poziomów zapewnienia zależy od jakości, niezależności i spójności audytów. Organizacje przeprowadzające audyty na poziomach 3 i 4 powinny mieć siedzibę w Unii Europejskiej, pozostawać pod europejską kontrolą oraz posiadać w UE kluczowy personel odpowiedzialny za realizację tych zadań.

Na poziomie Unii należy ustanowić jednolite wymogi akredytacyjne oraz przejrzysty europejski rejestr organizacji audytujących. Ograniczyłoby to możliwość arbitrażu regulacyjnego między państwami członkowskimi i ryzyko wydawania certyfikatów według różnych standardów jakości i wiarygodności.

System powinien umożliwiać przeprowadzanie niezapowiedzianych audytów oraz testowanie techniczne deklarowanych mechanizmów separacji, ciągłości działania i kontroli. Oceny nie powinny opierać się wyłącznie na dokumentacji przekazanej przez dostawcę.

Dostawcy powinni być również zobowiązani do zgłaszania nakazów dostępu do danych, prób wymuszenia przerwania lub ograniczenia świadczenia usługi oraz innych żądań organów państw trzecich mogących wpłynąć na bezpieczeństwo, dostępność lub kontrolę nad usługą. Obowiązek ten powinien dotyczyć zarówno samego dostawcy, jak i wszystkich podmiotów z jego grupy uczestniczących w świadczeniu usługi.

2. Zamówienia publiczne jako instrument polityki przemysłowej

Zamówienia publiczne powinny służyć tworzeniu przewidywalnego popytu na rozwiązania rozwijane i kontrolowane w Europie. Bez odpowiednich mechanizmów po stronie popytu projektowana regulacja może doprowadzić do zwiększenia liczby dostępnych certyfikatów i mocy obliczeniowych w Europie, nie zmieniając jednak udziału europejskich dostawców w rynku.

Kryterium unijnej wartości dodanej powinno mieć zastosowanie do wszystkich istotnych postępowań dotyczących usług chmurowych i AI, a nie wyłącznie do postępowań

formalnie klasyfikowanych jako zamówienia innowacyjne. O jego zastosowaniu powinny decydować znaczenie i przedmiot zamówienia, a nie jego formalna kwalifikacja.

Należy usunąć ograniczenie, zgodnie z którym kryterium unijnej wartości dodanej nie może przesądzać o wyniku postępowania. W zamówieniach strategicznych kryterium to powinno odpowiadać za co najmniej 20–30% łącznej oceny oferty.

Przy jego ocenie należy brać pod uwagę europejską kontrolę nad dostawcą, własność intelektualną, udział działalności badawczo-rozwojowej prowadzonej w Europie, lokalizację kluczowych kompetencji oraz wkład dostawcy w europejski łańcuch wartości.

W strategicznych zastosowaniach sektora publicznego powinien obowiązywać mechanizm preferencji europejskiej lub zasada European First. Jeżeli dostępna jest funkcjonalnie porównywalna oferta dostawcy znajdującego się pod europejską kontrolą, jej wybór powinien być rozwiązaniem domyślnym. Odstąpienie od tej zasady powinno wymagać pisemnego, publicznie dostępnego uzasadnienia.

Rozporządzenie powinno również ustanowić wiążący cel, zgodnie z którym do 2034 r. co najmniej 50% publicznych wydatków na usługi chmurowe powinno trafiać do dostawców znajdujących się pod europejską kontrolą. Postępy w realizacji tego celu powinny być monitorowane na poziomie Unii i państw członkowskich oraz uwzględniane w krajowych strategiach zakupowych.

Duże zamówienia powinny co do zasady być dzielone na części i dopuszczać architektury wielodostawcze. Zamawiający powinien mieć możliwość odstąpienia od tych zasad wyłącznie wtedy, gdy wykaże, że podział zamówienia lub zastosowanie architektury wielodostawczej byłoby nieuzasadnione technicznie lub ekonomicznie.

Takie podejście ułatwiłoby europejskim dostawcom udział w dużych postępowaniach, zmniejszało uzależnienie od pojedynczych dostawców oraz zwiększało możliwość przenoszenia obciążeń, zastępowania usług i zachowania ciągłości operacyjnej.

3. Europejska autonomia infrastrukturalna i inwestycyjna

Zwiększenie mocy centrów danych w Unii Europejskiej jest potrzebne, ale nie powinno być automatycznie utożsamiane ze wzrostem europejskiej autonomii technologicznej. Infrastruktura znajdująca się w UE może pozostawać pod kontrolą podmiotów z państw trzecich, wykorzystywać technologie rozwijane poza Europą i wzmacniać pozycję rynkową pozaeuropejskich dostawców.

Uzyskanie statusu strategicznego projektu centrum danych powinno wymagać mierzalnego wkładu w europejską suwerenność technologiczną. Samo wniesienie kapitału

lub zwiększenie dostępnej mocy obliczeniowej na terenie UE nie powinno być wystarczające.

Wsparcie publiczne powinno służyć zwiększaniu europejskiej własności, kontroli i zdolności technologicznych, a nie wyłącznie zwiększaniu mocy zlokalizowanych w Unii.

Preferencyjne finansowanie, dostęp do terenów, przyspieszone procedury wydawania pozwoleń oraz wsparcie w uzyskaniu dostępu do energii powinny być powiązane albo z europejską kontrolą nad infrastrukturą, albo z długoterminowym zobowiązaniem do przeznaczenia istotnej części mocy obliczeniowej dla europejskich dostawców i odbiorców strategicznych.

Ocena projektu powinna brać pod uwagę udział europejskiej wartości dodanej, w szczególności:

- badania i rozwój prowadzone w Europie;
- europejski personel i kompetencje;
- wykorzystanie europejskiego oprogramowania i sprzętu;
- energię pozyskiwaną w Europie;
- wkład projektu w europejską bazę podatkową;
- udział lokalnych i europejskich podwykonawców.

Beneficjent wsparcia dla projektu strategicznego powinien wykazać, w jaki sposób inwestycja zmniejsza zależności technologiczne Europy. Fundusze europejskie nie powinny wspierać projektów, które jedynie przenoszą geograficznie infrastrukturę kontrolowaną z państw trzecich lub prowadzą do dalszego wzrostu udziału pozaeuropejskich dostawców w rynku.

4. Rozszerzenie systemu na krytyczne sektory prywatne

Proponowany system nie powinien ograniczać się do administracji publicznej. Znaczna część krytycznych danych, infrastruktury i usług jest przetwarzana lub obsługiwana przez podmioty prywatne. Pozostawienie stosowania poziomów zapewnienia wyłącznie ich dobrowolnej decyzji może prowadzić do stosowania różnych standardów ochrony wobec porównywalnych systemów i danych.

Obowiązkowe oceny ryzyka powinny obejmować podmioty kluczowe w rozumieniu dyrektywy NIS2, co najmniej w sektorach ochrony zdrowia, energetyki, finansów, telekomunikacji, przestrzeni kosmicznej i obronności.

Dla określonych kategorii zastosowań krytycznych należy ustanowić minimalne unijne poziomy zapewnienia. Wymagany poziom powinien zależeć od rodzaju danych, funkcji systemu, konsekwencji przerwania świadczenia usługi oraz stopnia zależności technologicznej, niezależnie od tego, czy system jest obsługiwany przez podmiot publiczny, czy prywatny.

5. Mierzenie rzeczywistej zmiany rynku

Skuteczności nowych regulacji nie należy oceniać na podstawie liczby wydanych certyfikatów. Certyfikacja jest narzędziem realizacji polityki, a nie celem samym w sobie. Wzrost liczby usług objętych poziomami zapewnienia nie musi oznaczać wzmocnienia europejskich zdolności technologicznych ani ograniczenia koncentracji rynku.

Komisja Europejska oraz państwa członkowskie powinny monitorować w szczególności:

- udział europejskich dostawców w przychodach europejskiego rynku chmury i AI;
- udział mocy obliczeniowej znajdującej się pod europejską własnością i efektywną kontrolą;
- wartość zamówień publicznych udzielanych dostawcom znajdującym się pod europejską kontrolą;
- zmiany poziomu koncentracji europejskiego rynku chmury i AI.

Komisja powinna również monitorować, kto jest rzeczywistym ekonomicznym beneficjentem instrumentów przewidzianych w rozporządzeniu. Ocena powinna obejmować finansowanie publiczne, preferencyjne warunki inwestycyjne, przyspieszone procedury, instrumenty wsparcia związane z energią, zamówienia publiczne oraz status projektu strategicznego.

Bez takiego monitoringu wszystkie procesy regulacyjne przewidziane w projekcie mogą zostać formalnie wdrożone, podczas gdy udział dominujących dziś dostawców w rynku oraz zależności technologiczne Europy będą nadal rosły.

Podsumowanie

Cloud and AI Development Act może stać się jednym z kluczowych instrumentów rozwoju europejskiego ekosystemu chmury i AI. Aby osiągnąć ten cel, regulacja musi wyjść poza kryterium lokalizacji infrastruktury i formalne oznaczenia zgodności. Powinna premiować rzeczywistą europejską kontrolę, wykorzystywać zamówienia publiczne do kształtowania rynku, kierować wsparcie inwestycyjne do projektów ograniczających zależności technologiczne oraz tworzyć warunki do współpracy europejskich dostawców.

Skuteczności rozporządzenia nie należy oceniać przez pryzmat liczby certyfikowanych usług, wybudowanych centrów danych czy przeprowadzonych procesów oceny zgodności. Miarą sukcesu powinno być to, czy regulacja zwiększa udział dostawców znajdujących się pod europejską kontrolą, wzmacnia zdolność Europy do samodzielnego rozwijania i utrzymywania krytycznej infrastruktury cyfrowej oraz ogranicza strukturalne zależności w sektorach o strategicznym znaczeniu.

Europa potrzebuje czegoś więcej niż dodatkowych mocy w centrach danych. Potrzebuje dostawców dysponujących kompetencjami, technologią i zdolnościami operacyjnymi pozwalającymi samodzielnie rozwijać, utrzymywać i świadczyć kluczowe usługi.

Tylko wtedy proponowane regulacje będą mogły osiągnąć zakładany cel: stworzenie konkurencyjnego, odpornego i strategicznie autonomicznego europejskiego ekosystemu chmury i AI, zdolnego wspierać europejską gospodarkę cyfrową, sektor publiczny i infrastrukturę krytyczną.