KOMISJA
EUROPEJSKA

Bruksela, dnia 3.6.2026 r.
COM(2026) 502 final

ANNEXES 1 to 3

ZAŁĄCZNIKI

do

ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie ustanowienia ram środków na rzecz wzmocnienia europejskiego ekosystemu chmury obliczeniowej i sztucznej inteligencji (akt w sprawie rozwoju chmury i AI)

{SEC(2026) 502 final} - {SWD(2026) 502 final} - {SWD(2026) 503 final}

ZAŁĄCZNIK I

WIELKIE WYZWANIA

1. Wielkie wyzwanie nr 1: Zrównoważenie środowiskowe, wydajność i bezpieczeństwo unijnych ośrodków przetwarzania danych

Testowanie i wdrażanie technologii w ośrodkach przetwarzania danych w całej Unii w celu osiągnięcia poziomu efektywności energetycznej i efektywnego gospodarowania zasobami przewyższającego obecny stan techniki.

Obejmuje to osiągnięcie niższego wskaźnika efektywności zużycia energii (PUE) oraz zapewnienie znacznie wyższych wskaźników wykorzystania serwerów. Przykłady obejmują:

1) ***Obniżenie średniego wskaźnika efektywności zużycia energii (PUE)***: poprawa zrównoważenia środowiskowego i wydajności unijnych ośrodków przetwarzania danych w chmurze i przetwarzania brzegowego, aby osiągnąć średni wskaźnik efektywności zużycia energii (PUE) na poziomie 1,15 w całej Unii. Główne obszary priorytetowe obejmują wspieranie rozwoju:

   a) zaawansowanych technologii w zakresie efektywności energetycznej ośrodków przetwarzania danych, takich jak systemy chłodzenia czy odzysk ciepła odpadowego;

   b) kwantowych technologii obliczeniowych na potrzeby działania infrastruktury chmurowej i obliczeniowej;

   c) integracji z siecią energetyczną oraz zaawansowanych systemów zarządzania energią;

   d) linii pilotażowych służących walidacji energooszczędnych technologii nowej generacji w skali operacyjnej.

2) ***Podniesienie średnich wskaźników wykorzystania serwerów w ośrodkach przetwarzania danych:*** podniesienie średnich wskaźników wykorzystania serwerów w ośrodkach przetwarzania danych w całej Unii do poziomu 50 % poprzez wdrożenie, na przykład, technologii opartych na sztucznej inteligencji na potrzeby dynamicznego zarządzania wykorzystaniem serwerów, zarządzania obciążeniem w czasie rzeczywistym i planowania obciążenia, a także do równoważenia wykorzystania, kosztów energii, ograniczeń termicznych i wymagań dotyczących opóźnień.

3) ***Zwiększenie bezpieczeństwa i odporności ośrodków przetwarzania danych:*** zwiększenie bezpieczeństwa i odporności łańcucha wartości i dostaw w ośrodkach przetwarzania danych poprzez integrację technologii półprzewodnikowych i technologii kwantowych zaprojektowanych i wyprodukowanych w Unii, a także poprzez zwiększenie ich odporności na zagrożenia fizyczne i zagrożenia dla cyberbezpieczeństwa, w tym ataki ukierunkowane.

2. Wielkie wyzwanie nr 2: Stosy chmurowe

Tworzenie kompleksowych, obejmujących całe łańcuchy dostaw stosów sprzętu i oprogramowania do chmur obliczeniowych, w tym narzędzi sztucznej inteligencji, infrastruktury, usług i warstw zarządzania w celu wypełnienia krytycznych luk w zdolnościach Unii.

Obejmuje to budowę serwerów sztucznej inteligencji opartych na półprzewodnikach i technologiach kwantowych zaprojektowanych i wyprodukowanych w Unii, przeznaczonych

do rozproszonego i zdecentralizowanego przetwarzania w chmurze i przetwarzania brzegowego na potrzeby sztucznej inteligencji.

Programy pilotażowe mogłyby posłużyć do tego, aby wykazać zdolności europejskich otwartych stosów chmurowych w sektorach o znaczeniu strategicznym.

3. Wielkie wyzwanie nr 3: Pionierskie rozwiązania AI

Opracowanie nowej generacji modeli i systemów pionierskich rozwiązań multimodalnej AI oraz tworzenie nowatorskich zdolności.

Nacisk zostanie położony na projektowanie architektury i opracowywanie multimodalnych modeli i systemów nowej generacji, które przesuwają granice obecnych zdolności algorytmicznych w celu osiągnięcia najwyższej wydajności w zakresie zaawansowanego rozumowania, rozumienia międzymodalnego oraz zdolności agentowych; badanie nowatorskich podejść do efektywności modeli, modelowania kognitywnego oraz alternatywnych struktur obliczeniowych itp.

Potencjalne zastosowania mogłyby obejmować nauki podstawowe, takie jak odkrycia naukowe i interpretacja złożonych danych, a także opracowanie modeli świata służących usprawnieniu procesów rozumowania, zautomatyzowanej symulacji zarządzania oraz planowaniu.

4. Wielkie wyzwanie nr 4: Fizyczna AI

Opracowywanie zaawansowanych modeli i systemów fizycznej AI, które działają autonomicznie i bezpiecznie, zapewniając niezawodne zdolności w zakresie manipulacji i nawigacji w środowiskach nieustrukturyzowanych.

Nacisk zostanie położony na wspólne projektowanie oprogramowania i leżącej u jego podstaw architektury sprzętowej oraz na łączenie technik pionierskich rozwiązań AI z modelami świata wspierającymi rozumowanie fizyczne, co pozwoli zapewnić solidne zdolności w zakresie manipulacji, nawigacji i interakcji przy minimalnym nadzorze ze strony człowieka.

Potencjalne zastosowania mogłyby obejmować roboty autonomiczne, systemy przemysłowe i drony działające w dynamicznych warunkach rzeczywistych.

5. Wielkie wyzwanie nr 5: AI w przemyśle

Przyspieszenie rozwoju i wdrażania europejskiej AI w przemyśle w strategicznych sektorach Unii.

Nacisk zostanie położony na opracowanie europejskich modeli i systemów AI w przemyśle, zdolnych do obsługi zastosowań przemysłowych o wysokiej wartości. Takie modele i systemy powinny umożliwiać ich dostosowanie do konkretnych przypadków użycia i bezpieczne wdrażanie w poszczególnych sektorach.

Inicjatywy uruchomione w ramach tego wielkiego wyzwania powinny opierać się na wyspecjalizowanych zasobach obliczeniowych i zapleczu testowym, które są niezbędne do walidacji systemów AI w warunkach rzeczywistych, zanim zostaną one wdrożone na szeroką skalę i upowszechnione, w tym na szczeblu regionalnym i lokalnym.

W sektorze motoryzacyjnym inicjatywy te mogą ułatwić rozwój i wdrażanie innowacyjnych platform oprogramowania i modeli AI na potrzeby jazdy zautomatyzowanej, natomiast w produkcji mogą umożliwić tworzenie specjalistycznych modeli optymalizujących procesy produkcyjne. Innymi sektorami strategicznymi, które mogłyby odnieść korzyści

z zastosowania AI w przemyśle, mogą być między innymi opieka zdrowotna, energetyka, sektor rolno-spożywczy i obronność.

6. Wielkie wyzwanie nr 6: Europejskie modele przemysłowe oparte na współpracy

Opracowanie opartych na współpracy europejskich modeli i systemów AI w przemyśle dla sektorów strategicznych poprzez umożliwienie współpracy na europejską skalę przemysłową bez ujawniania szczególnie chronionych danych handlowych między uczestnikami.

Nacisk zostanie położony na zaawansowane technologie służące zachowaniu poufności. Mechanizmy te obejmują federacyjne i rozproszone podejścia do trenowania, w ramach których to algorytmy są dostarczane do danych zamiast przekazywania danych w sposób scentralizowany, bezpieczne środowiska wykonawcze, przetwarzanie oparte na szyfrowaniu, techniki anonimizacji i pseudonimizacji, podział uprawnień dostępowych oraz zabezpieczenia przed pozyskiwaniem szczególnie chronionych informacji handlowych z trenowanych modeli.

Sektory strategiczne, które mogłyby skorzystać z opartych na współpracy europejskich modeli i systemów AI w przemyśle, to między innymi przemysł lotniczy i kosmiczny, przemysł farmaceutyczny, cyberbezpieczeństwo, mobilność, pojazdy autonomiczne i drony, energetyka i obronność.

7. Wielkie wyzwanie nr 7: Platforma agentów AI

Opracowanie europejskich ram orkiestracji agentów AI, zapewniających niezbędne oprogramowanie pośredniczące na potrzeby niezawodnego i bezpiecznego wdrażania autonomicznych agentów na dużą skalę.

Nacisk zostanie położony na (i) badanie innowacyjnych paradygmatów technologicznych, które umożliwiają skuteczną współpracę wielu agentów AI, wykraczającą poza możliwości systemów działających samodzielnie, przy zachowaniu rygorystycznych standardów bezpieczeństwa; oraz (ii) stworzenie niezawodnych, opartych na chmurze otwartych platform przeznaczonych do zarządzania agentami AI na dużą skalę.

Potencjalne zastosowania mogą obejmować opiekę zdrowotną (np. wsparcie przy podejmowaniu decyzji klinicznych i koordynację badań), cyberbezpieczeństwo (np. wykrywanie zagrożeń i reagowanie na nie), a także nauki podstawowe.

8. Wielkie wyzwanie nr 8: AI w sektorze publicznym

Opracowywanie modeli i systemów AI w oparciu o wysokiej jakości dane pochodzące z sektora publicznego, ukierunkowane na dziedziny o kluczowym znaczeniu (takie jak opieka zdrowotna, administracja publiczna, prawo i zarządzanie kryzysowe, a także usługi użyteczności publicznej)

Nacisk zostanie położony na rozwiązania w zakresie usług publicznych, co do których oczekuje się, że będą miały znaczący pozytywny wpływ na usługi użyteczności publicznej o kluczowym znaczeniu i będą wykorzystywane różnych szczeblach organizacji sektora publicznego.

Jednym z celów będzie umożliwienie wymiany danych i opracowywania nowatorskich modeli w ramach krajowych usług użyteczności publicznej w celu zwiększenia wpływu na cały unijny sektor publiczny, w tym również w obszarach związanych z przetwarzaniem danych wrażliwych. Do osiągnięcia tego celu przyczynią się również ramy ochrony prywatności (takie jak uczenie federacyjne i generowanie wysokiej jakości danych syntetycznych), które umożliwiają trenowanie modeli bez naruszania poufności

podstawowych zbiorów danych, oraz działania mające na celu przyspieszenie upowszechnienia tych modeli, w tym na szczeblu regionalnym i lokalnym.

ZAŁĄCZNIK II

KRYTERIA DOTYCZĄCE UNIJNYCH POZIOMÓW UZASADNIENIA ZAUFANIA

W niniejszym załączniku określono kryteria, które muszą spełnić dostawcy usług chmurowych i świadczone przez nich usługi chmurowe, aby można było uznać, że oferowane przez nich usługi odpowiadają unijnym poziomom uzasadnienia zaufania 1, 2, 3 i 4. Do celów kryteriów dotyczących unijnych poziomów uzasadnienia zaufania 1, 2, 3 i 4 „oprogramowanie" w rozumieniu art. 3 pkt 4 rozporządzenia (UE) 2024/2847 wchodzi w zakres niniejszego załącznika i załącznika III do niniejszego rozporządzenia. „Sprzęt" w rozumieniu art. 3 pkt 5 rozporządzenia (UE) 2024/2847 nie wchodzi w zakres jego stosowania.

1. Unijny poziom uzasadnienia zaufania 1

1.1. W przypadku unijnego poziomu uzasadnienia zaufania 1 dostawcy usług chmurowych muszą spełniać łącznie następujące kryteria:

a) dostawca usług chmurowych ma siedzibę w Unii;

b) infrastruktura i aktywa dostawcy usług chmurowych, w tym jego podwykonawców zaangażowanych w świadczenie tych usług, znajdują się w Unii, chyba że wymóg wprowadzony przez organ sektora publicznego wyraźnie stanowi inaczej;

c) dane klientów, w tym metadane i dane telemetryczne, które są przetwarzane, przechowywane i przekazywane przez dostawcę usług chmurowych oraz przez podwykonawców zaangażowanych w świadczenie tych usług, pozostają wyłącznie na terytorium Unii w dowolnym momencie, w tym przed konfiguracją lub skorzystaniem z usługi, w trakcie konfiguracji lub korzystania z usługi lub po skonfigurowaniu lub skorzystaniu z usługi, chyba że wymóg wprowadzony przez organ sektora publicznego wyraźnie stanowi inaczej;

d) w przypadku gdy dostawca usług chmurowych zleca wsparcie techniczne i operacyjne lub pomoc techniczną i operacyjną – w tym w ramach wszelkich późniejszych umów dotyczących podzlecenia na zasadzie outsourcingu – zewnętrznym dostawcom usług spoza Unii, wdrażane są niezbędne środki prawne, techniczne i organizacyjne w celu zapewnienia identyfikowalności i bezpieczeństwa tych operacji oraz nadzoru nad tymi operacjami, a operacje te w żaden sposób nie naruszają autonomii operacyjnej dostawcy usług chmurowych;

e) dostawca usług chmurowych wykazuje, że usługa spełnia najnowocześniejsze standardy cyberbezpieczeństwa;

f) dostawca usług chmurowych zapewnia pełną przejrzystość w zakresie korzystania z usług podwykonawców. Dostawca usług chmurowych poddaje podwykonawców procedurze należytej staranności, nakłada na nich zobowiązania umowne i sprawuje nad nimi stały nadzór w celu wypełnienia obowiązków prawnych wynikających z prawa Unii;

g) W przypadku gdy dostawca usług chmurowych podlega kontroli państwa trzeciego lub podmiotu prawnego mającego siedzibę w państwie trzecim, dostawca usług chmurowych gwarantuje, że w tym państwie trzecim nie obowiązują żadne przepisy ani praktyki – co potwierdzają niezależne źródła – które wymagałyby od dostawcy usług chmurowych zgłaszania organom tego państwa trzeciego informacji o lukach w zabezpieczeniach oprogramowania, zanim zostanie stwierdzone, że luki te zostały wykorzystane.

1.2. W przypadku unijnego poziomu uzasadnienia zaufania 1 podwykonawcy, o których mowa w akapicie pierwszym, muszą być podwykonawcami będącymi osobami trzecimi, które pozostają w bezpośrednim stosunku umownym z dostawcą usług chmurowych i które są zaangażowane w świadczenie usług chmurowych.

2. Unijny poziom uzasadnienia zaufania 2

2.1. W przypadku unijnego poziomu uzasadnienia zaufania 2 dostawcy usług chmurowych muszą spełniać łącznie następujące kryteria:

a) audytowany dostawca i podwykonawcy zaangażowani w świadczenie usługi będącej przedmiotem audytu mają siedzibę w Unii;

b) infrastruktura, aktywa i personel audytowanego dostawcy, w tym jego podwykonawców zaangażowanych w świadczenie usługi, znajdują się w Unii;

c) dane klientów, w tym metadane i dane telemetryczne, które są przetwarzane, przechowywane i przekazywane przez audytowanego dostawcę oraz przez podwykonawców zaangażowanych w świadczenie usługi, pozostają wyłącznie na terytorium Unii w dowolnym momencie, w tym przed konfiguracją lub skorzystaniem z usługi, w trakcie konfiguracji lub korzystania z usługi lub po skonfigurowaniu lub skorzystaniu z usługi, chyba że wymóg wprowadzony przez organ sektora publicznego wyraźnie stanowi inaczej;

d) jeżeli organ sektora publicznego uzna, że konieczne jest nałożenie dodatkowych wymogów dotyczących weryfikacji personelu i posiadania obywatelstwa Unii, audytowany dostawca powinien zapewnić dostępność personelu spełniającego te wymogi;

e) usługa będąca przedmiotem audytu uzyskuje europejski certyfikat cyberbezpieczeństwa o co najmniej „istotnym” poziomie uzasadnienia zaufania w ramach europejskiego programu certyfikacji cyberbezpieczeństwa obejmującego usługi chmurowe, który ma zostać ustanowiony na mocy rozporządzenia (UE) 2019/881, pod warunkiem że taki program został ustanowiony na podstawie tego rozporządzenia i jest dostępny dla dostawców usług chmurowych. Do czasu ustanowienia takiego systemu stosuje się krajowe programy certyfikacji cyberbezpieczeństwa, jeżeli takie istnieją. W przypadku braku unijnych lub krajowych programów certyfikacji cyberbezpieczeństwa audytowany dostawca ma obowiązek wykazać, że usługa spełnia najwyższe normy cyberbezpieczeństwa zgodnie z mającym zastosowanie prawem Unii;

f) dane wygenerowane w wyniku korzystania z usługi będącej przedmiotem audytu nie są wykorzystywane do trenowania ani dostrajania jakiegokolwiek systemu AI obsługiwanego przez państwo trzecie lub podmiot prawny mający siedzibę w państwie trzecim i w żadnym wypadku nie są przekazywane poza Unię;

g) jeżeli audytowany dostawca i podwykonawcy zaangażowani w świadczenie usługi będącej przedmiotem audytu podlegają kontroli państwa trzeciego lub podmiotu prawnego mającego siedzibę w państwie trzecim, wykazują oni, że wdrożono niezbędne środki prawne, techniczne i organizacyjne gwarantujące, że:

   i. kontrola państwa trzeciego lub podmiotu prawnego mającego siedzibę w państwie trzecim nad audytowanym dostawcą nie jest sprawowana w sposób, który odbiera dostawcy swobodę świadczenia usługi lub ogranicza możliwość jej świadczenia, nakłada ograniczenia dotyczące infrastruktury, aktywów i personelu niezbędnych do świadczenia usługi lub osłabia zdolności

i podważa normy niezbędne do świadczenia usługi będącej przedmiotem audytu;

ii. państwo trzecie lub podmiot prawny mający siedzibę w państwie trzecim nie ma dostępu do danych klientów;

iii. państwo trzecie lub podmiot prawny mający siedzibę w państwie trzecim nie ma możliwości zakłócania ciągłości świadczenia usług lub obniżania jakości usługi;

iv. kontrola państwa trzeciego lub podmiotu prawnego mającego siedzibę w państwie trzecim nad audytowanym dostawcą nie jest sprawowana w sposób, który zobowiązuje audytowanego dostawcę do wdrożenia, egzekwowania, wprowadzenia w życie i stosowania się do środków ograniczających, takich jak systemy sankcji, embarga lub wszelkie równoważne środki prawne lub administracyjne przyjęte przez państwo trzecie, chyba że takie środki są uzasadnione na mocy prawa krajowego państw członkowskich lub prawa Unii;

h) wsparcie techniczne i operacyjne lub pomoc techniczna i operacyjna w związku z usługą będącą przedmiotem audytu, w tym późniejsze ustalenia dotyczące podzlecenia na zasadzie outsourcingu, są inicjowane i realizowane wyłącznie w Unii;

i) audytowany dostawca wykazuje, że wprowadzono następujące środki dotyczące łańcucha dostaw oprogramowania:

i. kompletne i aktualne zestawienie podstawowych materiałów do produkcji oprogramowania (SBOM), zgodnie z definicją w art. 3 pkt 39 rozporządzenia (UE) 2024/2847, oraz wykaz zidentyfikowanych zależności związanych ze świadczeniem usługi są dokumentowane i udostępnia się je organizacji audytowej;

ii. w przypadku gdy komponenty oprogramowania, zgodnie z definicją w art. 3 pkt 6 rozporządzenia (UE) 2024/2847, lub produkty są dostarczane i licencjonowane przez podmiot prawny mający siedzibę w państwie trzecim lub stanowią własność takiego podmiotu, wdraża się i dokumentuje środki kontroli mające na celu zablokowanie wszelkich funkcji zdalnych, które mogłyby w istotny sposób ingerować w urządzenie, system lub oprogramowanie lub zakłócać ich działanie (w tym podczas aktualizacji), oraz w celu zapewnienia, aby istotne dla bezpieczeństwa komponenty pochodzące od producentów oprogramowania z państw trzecich, zgodnie z definicją w art. 3 pkt 13 rozporządzenia (UE) 2024/2847, podlegały audytom kodu źródłowego oraz posiadały udokumentowany plan migracji na wypadek upadłości dostawcy lub nałożenia ograniczeń przez państwo trzecie;

iii. w przypadku gdy dostawca usług chmurowych podlega kontroli państwa trzeciego lub podmiotu prawnego mającego siedzibę w państwie trzecim, dostawca usług chmurowych gwarantuje, że w tym państwie trzecim nie obowiązują żadne przepisy i praktyki – co potwierdzają niezależne źródła – które wymagałyby od dostawcy usług chmurowych zgłaszania organom tego państwa trzeciego informacji o lukach w zabezpieczeniach oprogramowania, zanim zostanie stwierdzone, że luki te zostały wykorzystane;

j) w przypadku gdy do świadczenia usługi wykorzystywane jest oprogramowanie udostępnione na podstawie licencji otwartego oprogramowania, audytowany dostawca wykazuje, że wdrożył i udokumentował odpowiednie środki kontroli

zapobiegające korzystaniu z jakichkolwiek zdalnych funkcji lub mechanizmów, które mogłyby zostać wykorzystane do istotnej ingerencji w urządzenie, system lub oprogramowanie lub do zakłócenia ich działania;

k) w zakresie, w jakim audytowany dostawca świadczy usługi na całym świecie, a jego jednostka zależna działa w państwie trzecim, audytowany dostawca wdrożył niezbędne środki w celu zapewnienia i egzekwowania skutecznego rozdzielenia prawnego, technicznego i organizacyjnego między unijną jednostką dominującą a każdą taką jednostką zależną w państwie trzecim.

2.2. W przypadku unijnego poziomu uzasadnienia zaufania 2 podwykonawcy, o których mowa w akapicie pierwszym, muszą być podwykonawcami będącymi osobami trzecimi, które pozostają w bezpośrednim stosunku umownym z dostawcą usług chmurowych i które są zaangażowane w świadczenie usług chmurowych.

3. Unijny poziom uzasadnienia zaufania 3

3.1. W przypadku unijnego poziomu uzasadnienia zaufania 3 dostawcy usług chmurowych muszą spełniać łącznie następujące kryteria:

a) audytowany dostawca i podwykonawcy zaangażowani w świadczenie usługi będącej przedmiotem audytu mają siedzibę w Unii;

b) infrastruktura, aktywa i personel audytowanego dostawcy, w tym podwykonawców zaangażowanych w świadczenie usługi, znajdują się w Unii;

c) dane klientów, w tym metadane i dane telemetryczne, które są przetwarzane, przechowywane i przekazywane przez audytowanego dostawcę oraz przez podwykonawców zaangażowanych w świadczenie tych usług, pozostają wyłącznie na terytorium Unii w dowolnym momencie, w tym przed konfiguracją lub skorzystaniem z usługi, w trakcie konfiguracji lub korzystania z usługi lub po skonfigurowaniu lub skorzystaniu z usługi, chyba że wymóg wprowadzony przez organ sektora publicznego wyraźnie stanowi inaczej;

d) personel, w tym personel podwykonawców, zaangażowany w świadczenie usługi będącej przedmiotem audytu składa się z obywateli Unii, którzy w stosownych przypadkach muszą również posiadać niezbędne krajowe poświadczenie bezpieczeństwa wydane przez państwo członkowskie w zakresie postępowania z informacjami niejawnymi w rozumieniu art. 2 pkt 21 rozporządzenia (UE) 2021/697;

e) usługa będąca przedmiotem audytu uzyskuje europejski certyfikat cyberbezpieczeństwa o co najmniej „istotnym” poziomie uzasadnienia zaufania w ramach europejskiego programu certyfikacji cyberbezpieczeństwa obejmującego usługi chmurowe, który ma zostać ustanowiony na mocy rozporządzenia (UE) 2019/881, pod warunkiem że taki program został ustanowiony na podstawie tego rozporządzenia i jest dostępny dla dostawców usług chmurowych. Do czasu ustanowienia takiego systemu stosuje się krajowe programy certyfikacji cyberbezpieczeństwa, jeżeli takie istnieją. W przypadku braku unijnych lub krajowych programów certyfikacji cyberbezpieczeństwa audytowany dostawca ma obowiązek wykazać, że usługa spełnia najwyższe normy cyberbezpieczeństwa zgodnie z mającym zastosowanie prawem Unii;

f) dane wygenerowane w wyniku korzystania z usługi będącej przedmiotem audytu nie są wykorzystywane do trenowania ani dostrajania jakiegokolwiek systemu AI

obsługiwanego przez państwo trzecie lub podmiot prawny mający siedzibę w państwie trzecim i w żadnym wypadku nie są przekazywane poza Unię;

g) audytowany dostawca i podwykonawcy zaangażowani w świadczenie usługi będącej przedmiotem audytu nie podlegają kontroli państwa trzeciego ani podmiotu prawnego mającego siedzibę w państwie trzecim. Na zasadzie odstępstwa od tego kryterium dostawca usług chmurowych i jego podwykonawcy zaangażowani w świadczenie usługi będącej przedmiotem audytu, którzy podlegają kontroli państwa trzeciego lub podmiotu prawnego mającego siedzibę w państwie trzecim, mogą zostać poddani audytowi pod kątem unijnego poziomu uzasadnienia zaufania 3, jeżeli Komisja przyjęła akt wykonawczy na podstawie art. 19. W przypadku gdy Komisja przyjęła akt wykonawczy na podstawie art. 19, audytowany dostawca i podwykonawcy zaangażowani w świadczenie usługi będącej przedmiotem audytu muszą również wykazać, że wdrożono niezbędne środki prawne, techniczne i organizacyjne gwarantujące, że:

   i. kontrola państwa trzeciego lub podmiotu prawnego mającego siedzibę w państwie trzecim nad audytowanym dostawcą nie jest sprawowana w sposób, który odbiera dostawcy swobodę świadczenia usługi lub ogranicza możliwość jej świadczenia, nakłada ograniczenia dotyczące infrastruktury, aktywów i personelu niezbędnych do świadczenia usługi lub osłabia zdolności i podważa normy niezbędne do świadczenia usługi będącej przedmiotem audytu. Audytowany dostawca powinien umożliwić rozsądny dostęp do kodu;

   ii. państwo trzecie lub podmiot prawny mający siedzibę w państwie trzecim nie ma dostępu do danych klientów;

   iii. państwo trzecie lub podmiot prawny mający siedzibę w państwie trzecim nie ma możliwości zakłócania ciągłości świadczenia usług lub obniżania jakości usługi;

   iv. kontrola państwa trzeciego lub podmiotu prawnego mającego siedzibę w państwie trzecim nad audytowanym dostawcą nie jest sprawowana w sposób, który zobowiązuje audytowanego dostawcę do wdrożenia, egzekwowania, wprowadzenia w życie i stosowania się do środków ograniczających, takich jak systemy sankcji, embarga lub wszelkie równoważne środki prawne lub administracyjne przyjęte przez państwo trzecie, chyba że takie środki są uzasadnione na mocy prawa krajowego państw członkowskich lub prawa Unii;

h) wsparcie techniczne i operacyjne lub pomoc techniczna i operacyjna w związku z usługą będącą przedmiotem audytu, w tym późniejsze ustalenia dotyczące podzlecenia na zasadzie outsourcingu, są inicjowane i realizowane wyłącznie w Unii przez personel składający się z rezydentów Unii oraz przez osoby trzecie, które nie podlegają kontroli państwa trzeciego lub podmiotu prawnego mającego siedzibę w państwie trzecim;

i) audytowany dostawca wykazuje, że wprowadzono następujące środki dotyczące łańcucha dostaw oprogramowania:

   i. kompletne i aktualne zestawienie podstawowych materiałów do produkcji oprogramowania oraz wykaz zidentyfikowanych zależności istotnych dla świadczenia usługi są dokumentowane i udostępnia się je organizacji audytowej;

ii. w przypadku gdy komponenty oprogramowania lub produkty są dostarczane i licencjonowane przez podmiot prawny mający siedzibę w państwie trzecim lub stanowią własność takiego podmiotu, wdraża się i dokumentuje środki kontroli mające na celu zablokowanie wszelkich funkcji zdalnych, które mogłyby w istotny sposób ingerować w urządzenie, system lub oprogramowanie lub zakłócać ich działanie (w tym podczas aktualizacji), oraz w celu zapewnienia, aby istotne dla bezpieczeństwa komponenty pochodzące od producentów z państw trzecich podlegały audytom kodu źródłowego oraz posiadały udokumentowany plan migracji na wypadek upadłości dostawcy lub nałożenia ograniczeń przez państwo trzecie;

iii. w przypadku gdy dostawca usług chmurowych podlega kontroli państwa trzeciego lub podmiotu prawnego mającego siedzibę w państwie trzecim, dostawca usług chmurowych gwarantuje, że w tym państwie trzecim nie obowiązują żadne przepisy ani praktyki – co potwierdzają niezależne źródła – które wymagałyby od dostawcy usług chmurowych zgłaszania organom tego państwa trzeciego informacji o lukach w zabezpieczeniach oprogramowania, zanim zostanie stwierdzone, że luki te zostały wykorzystane;

j) w przypadku gdy do świadczenia usługi wykorzystywane jest oprogramowanie udostępnione na podstawie licencji otwartego oprogramowania, audytowany dostawca wykazuje, że wdrożył i udokumentował odpowiednie środki kontroli zapobiegające korzystaniu z jakichkolwiek zdalnych funkcji lub mechanizmów, które mogłyby zostać wykorzystane do istotnej ingerencji w urządzenie, system lub oprogramowanie lub do zakłócenia ich działania;

k) w zakresie, w jakim audytowany dostawca świadczy swoje usługi poza terytorium Unii, a jego jednostka zależna działa w państwie trzecim, audytowany dostawca wykazuje, że wdrożył niezbędne środki w celu zapewnienia i egzekwowania skutecznego rozdzielenia prawnego, technicznego i organizacyjnego między unijną jednostką dominującą a każdą taką jednostką zależną w państwie trzecim.

3.2. W przypadku unijnego poziomu uzasadnienia zaufania 3 podwykonawcy, o których mowa w akapicie pierwszym, muszą być podwykonawcami będącymi osobami trzecimi, które pozostają w bezpośrednim stosunku umownym z dostawcą usług chmurowych i które są zaangażowane w świadczenie usługi chmurowej oraz które mogą wymagać dostępu do informacji niejawnych lub szczególnie chronionych w rozumieniu w art. 2 pkt 22 rozporządzenia (UE) 2021/697.

4. Unijny poziom uzasadnienia zaufania 4

4.1. W przypadku unijnego poziomu uzasadnienia zaufania 4 dostawcy usług chmurowych muszą spełniać łącznie następujące kryteria:

a) audytowany dostawca i podwykonawcy zaangażowani w świadczenie usługi będącej przedmiotem audytu mają siedzibę w Unii;

b) infrastruktura, aktywa i personel audytowanego dostawcy, w tym podwykonawców zaangażowanych w świadczenie usługi, znajdują się w Unii;

c) dane klientów, w tym metadane i dane telemetryczne, które w wyniku oceny ryzyka uznano za wrażliwe, a które są przetwarzane, przechowywane i przekazywane przez audytowanego dostawcę i podwykonawców zaangażowanych w świadczenie usługi, pozostają wyłącznie w Unii w dowolnym momencie, w tym przed konfiguracją lub skorzystaniem z usługi, w trakcie konfiguracji lub korzystania z usługi lub po skonfigurowaniu lub skorzystaniu z usługi;

d) personel, w tym personel podwykonawców, zaangażowany w świadczenie usługi będącej przedmiotem audytu składa się z obywateli Unii, którzy w stosownych przypadkach muszą również posiadać niezbędne krajowe poświadczenie bezpieczeństwa wydane przez państwo członkowskie w zakresie postępowania z informacjami niejawnymi;

e) usługa będąca przedmiotem audytu uzyskuje europejski certyfikat cyberbezpieczeństwa o co najmniej „wysokim" poziomie uzasadnienia zaufania w ramach europejskiego programu certyfikacji cyberbezpieczeństwa obejmującego usługi chmurowe, który ma zostać ustanowiony na mocy rozporządzenia (UE) 2019/881, pod warunkiem że taki program został ustanowiony na podstawie tego rozporządzenia i jest dostępny dla dostawców usług chmurowych. Do czasu ustanowienia takiego systemu stosuje się krajowe programy certyfikacji cyberbezpieczeństwa, jeżeli takie istnieją. W przypadku braku unijnych lub krajowych programów certyfikacji cyberbezpieczeństwa audytowany dostawca ma obowiązek wykazać, że usługa spełnia najwyższe normy cyberbezpieczeństwa zgodnie z mającym zastosowanie prawem Unii;

f) dane wygenerowane w wyniku korzystania z usługi będącej przedmiotem audytu nie są wykorzystywane do trenowania ani dostrajania jakiegokolwiek systemu AI obsługiwanego przez państwo trzecie lub podmiot prawny mający siedzibę w państwie trzecim i w żadnym wypadku nie są przekazywane poza Unię;

g) audytowany dostawca i podwykonawcy zaangażowani w świadczenie usługi będącej przedmiotem audytu nie podlegają kontroli państwa trzeciego ani podmiotu prawnego mającego siedzibę w państwie trzecim;

h) wsparcie techniczne i operacyjne lub pomoc techniczna i operacyjna w związku z usługą będącą przedmiotem audytu, w tym późniejsze ustalenia dotyczące podzlecenia na zasadzie outsourcingu, są inicjowane i realizowane wyłącznie w Unii przez personel składający się z rezydentów Unii oraz przez osoby trzecie, które nie podlegają kontroli państwa trzeciego lub podmiotu prawnego mającego siedzibę w państwie trzecim;

i) audytowany dostawca wykazuje, że wprowadzono następujące środki dotyczące łańcucha dostaw oprogramowania:

   i. kompletne i aktualne zestawienie podstawowych materiałów do produkcji oprogramowania oraz wykaz zidentyfikowanych zależności istotnych dla świadczenia usługi są dokumentowane i udostępnia się je organizacji audytowej;

   ii. środki mające na celu zachowanie skutecznej kontroli nad komponentami oprogramowania lub produktami poprzez wykazanie, że państwo trzecie lub podmiot prawny mający siedzibę w państwie trzecim nie posiada ani nie sprawuje skutecznej kontroli nad projektowaniem, opracowywaniem, konserwacją i rozwojem tych komponentów lub produktów. Skuteczna kontrola obejmuje zdolność do wywierania istotnego wpływu na rozwój techniczny, priorytety w zakresie utrzymania, działania zaradcze na rzecz bezpieczeństwa oraz długoterminową ciągłość działania komponentu;

j) w przypadku gdy wykorzystywane jest oprogramowanie udostępnione na podstawie licencji otwartego oprogramowania, audytowany dostawca wykazuje, że wdrożył i udokumentował odpowiednie środki kontroli zapobiegające korzystaniu z jakichkolwiek zdalnych funkcji lub mechanizmów, które mogłyby zostać

wykorzystane do istotnej ingerencji w urządzenie, system lub oprogramowanie lub do zakłócenia ich działania;

k) w zakresie, w jakim audytowany dostawca świadczy swoje usługi poza terytorium Unii, a jego jednostka zależna działa w państwie trzecim, audytowany dostawca wykazuje, że wdrożył niezbędne środki w celu zapewnienia i egzekwowania skutecznego rozdzielenia prawnego, technicznego i organizacyjnego między unijną jednostką dominującą a każdą taką jednostką zależną w państwie trzecim.

4.2. W przypadku unijnego poziomu uzasadnienia zaufania 4 podwykonawcy, o których mowa w akapicie pierwszym, muszą być podwykonawcami będącymi osobami trzecimi, które pozostają w bezpośrednim stosunku umownym z dostawcą usług chmurowych, są zaangażowane w świadczenie usługi chmurowej oraz mogą wymagać dostępu do informacji niejawnych lub szczególnie chronionych na potrzeby świadczenia tej usługi.

ZAŁĄCZNIK III

DOWODY AUDYTOWE DO CELÓW PROCEDURY AUDYTU

Oceniając zgodność usługi będącej przedmiotem audytu z mającymi zastosowanie kryteriami audytu określonymi w załączniku II, organizacje audytowe powinny zwrócić się do audytowanego dostawcy o przedstawienie dowodów audytowych wymienionych w niniejszym załączniku.

Niniejszy załącznik ma charakter orientacyjny i nie ogranicza zakresu dowodów, o które mogą wystąpić lub które mogą uwzględnić organizacje audytowe. Audytorzy mogą zwracać się o wszelkie dodatkowe informacje niezbędne do zapewnienia kompleksowej i dokładnej oceny zgodności w celu przeprowadzenia audytów. Chociaż wymagane dowody mogą być takie same, aspekty, które należy przeanalizować, będą się różnić w zależności od kryteriów poziomu uzasadnienia zaufania i ich surowości.

1. Kryterium audytu A – Siedziba w Unii

Organizacja audytowa powinna ocenić kryterium audytu wymienione w załączniku II, lit. a) dla unijnych poziomów uzasadnienia zaufania 2, 3 i 4 w oparciu o następujące ustalenia:

1) Wszelkie dowody potwierdzające, że audytowany dostawca został zarejestrowany na mocy prawa jednego z państw członkowskich Unii lub w inny sposób utworzony zgodnie z prawem spółek jednego z państw członkowskich Unii.

2) Wszelkie dowody potwierdzające, że siedziba statutowa, zarząd i główne miejsce prowadzenia działalności audytowanego dostawcy znajduje się w Unii.

3) Organizacja audytowa powinna zweryfikować unijne ramy prawne mające zastosowanie do audytowanego dostawcy i sprawdzić, czy jego miejsce prowadzenia działalności jest rzeczywiste i trwałe, czy też audytowany dostawca kwalifikuje się jako dostawca spoza UE oferujący usługi w Unii.

4) Organizacja audytowa powinna sprawdzić, czy dostawca jest zgodnie z prawem zarejestrowany w jednym z państw członkowskich Unii. Dowodem na to mogą być między innymi krajowe wyciągi z rejestru przedsiębiorstw, dokumentacja potwierdzająca rezydencję podatkową, zezwolenia na prowadzenie działalności, rejestracja jako płatnik VAT, a także sprawdzenie, czy dostawca usług jest zarejestrowany w systemie integracji rejestrów przedsiębiorstw (BRIS) i w systemie wymiany informacji o VAT (VIES).

5) Organizacja audytowa powinna zweryfikować, czy audytowany dostawca prowadzi stałą i faktyczną działalność na terenie Unii. Organizacja audytowa powinna zatem sprawdzić, czy:

   a) w UE znajdują się fizyczne biura lub lokale, w których dostawca prowadzi działalność (np. na podstawie umów najmu, rachunków za media lub dokumentów dotyczących nieruchomości);

   b) stały personel znajduje się w Unii i czynności w zakresie obsługi klienta są prowadzone w Unii (na przykład na podstawie umów o pracę, dokumentacji płacowej, kart ewidencji czasu pracy);

   c) działania związane z wykonywaniem umów są prowadzone w Unii (na przykład na podstawie dokumentacji dotyczącej zarządzania działalnością, rejestrów zgłoszeń incydentów);

d) operacje bankowe i księgowe wykonywane są wyłącznie w Unii (na przykład na podstawie sprawozdań finansowych i obowiązkowych sprawozdań z audytów).

6) Organizacja audytowa powinna sprawdzić, czy w państwach członkowskich UE faktycznie działają jednostki lub oddziały dostawcy (na przykład na podstawie umów najmu, rachunków za media, dokumentów dotyczących nieruchomości, umów o pracę, kart ewidencji czasu pracy, dokumentacji płacowej lub zamówień).

2. Kryterium audytu B – Usytuowanie infrastruktury, aktywów i personelu

Organizacja audytowa powinna ocenić kryterium audytu wymienione w załączniku II, lit. b) dla unijnych poziomów uzasadnienia zaufania 2, 3 i 4 w oparciu o następujące ustalenia:

1) Usytuowanie infrastruktury

a) Wykaz zawierający istotne informacje dotyczące usytuowania infrastruktury oraz miejsc przechowywania danych wykorzystywanych do świadczenia usługi będącej przedmiotem audytu. Wykaz ten powinien zawierać dokładną lokalizację infrastruktury (numer budynku, ulicę, miejscowość, kod pocztowy i państwo) na potwierdzenie, że wszystkie elementy niezbędne do świadczenia usługi będącej przedmiotem audytu znajdują się na terytorium Unii. Obejmuje to lokalizację serwerów głównych, serwerów zapasowych, systemów odzyskiwania danych po awarii oraz miejsc przechowywania rejestrów.

b) Wszelkie inne dowody potwierdzające, że infrastruktura informatyczna znajduje się w Unii, takie jak umowy najmu, akty własności, umowy serwisowe, umowy o świadczenie usług, rejestry dostępu do obiektów.

c) Schematy sieciowe i dokumenty dotyczące architektury ilustrujące wyłączne wykorzystanie unijnej infrastruktury do przechowywania i przetwarzania danych, w tym danych zapasowych i danych powielonych.

2) Usytuowanie aktywów

a) Wykaz i istotne szczegóły dotyczące aktywów wykorzystywanych do świadczenia usługi będącej przedmiotem audytu, takie jak rejestr aktywów.

b) Dowody potwierdzające, że serwery, sprzęt i aktywa operacyjne znajdują się na terenie Unii, takie jak dokumentacja identyfikująca serwer i jego lokalizację, faktury zakupu, dowody dostawy, umowy licencyjne, umowy subskrypcji lub faktury za zakup lub subskrypcję oprogramowania, faktury za dostawę sprzętu.

c) Dowody potwierdzające, że zdolności w zakresie świadczenia usług znajdują się na terenie Unii, takie jak dokumentacja wdrożenia, rejestry instalacji, sprawozdania dotyczące statusu usługi, raporty konfiguracyjne, wyniki monitorowania, rejestry administracyjne dokumentujące korzystanie z usługi.

3) Usytuowanie personelu

a) Wykaz i odpowiednie dane szczegółowe dotyczące personelu zaangażowanego w świadczenie usługi będącej przedmiotem audytu.

b) Dowody potwierdzające, że personel zaangażowany w świadczenie usługi będącej przedmiotem audytu znajduje się w Unii, takie jak umowy o pracę, dokumentacja płacowa, karty ewidencji czasu pracy, rejestry czynności

i schematy organizacyjne przedstawiające pracowników w Unii, którym powierzono obowiązki operacyjne.

4) Ustalenia dotyczące infrastruktury, aktywów i personelu

a) Organizacja audytowa powinna również ustalić, czy:

i. w przypadku takiej infrastruktury, aktywów lub personelu ma miejsce przechowanie, przekazywanie, przetwarzanie i dostęp do danych klientów lub innego rodzaju postępowanie z danymi klientów;

ii. za pośrednictwem takiej infrastruktury, aktywów lub personelu zapewnia się lub umożliwia (lub można umożliwić) dostęp administracyjny do danych klientów, kontrolę nad danymi klientów, ich konfigurację lub wglądu w takie dane;

iii. w przypadku naruszenia bezpieczeństwa, nieprawidłowej konfiguracji, niedostępności lub zakłóceń takiej infrastruktury, aktywów lub personelu mogłoby dojść do zakłócenia działania lub niedostępności usługi będącej przedmiotem audytu.

***UWAGA**: „infrastruktura" oznacza infrastrukturę fizyczną, w tym między innymi infrastrukturę ośrodka przetwarzania danych lub infrastrukturę kolokacyjną, sieci, systemy chłodzenia i systemy informatyczne, które umożliwiają zarządzanie ośrodkiem przetwarzania danych.*

„Aktywa" oznaczają sprzęt i oprogramowanie, w tym między innymi biblioteki, sieć wewnętrzną niezbędną do komunikacji między komponentami oprogramowania oraz materiały kryptograficzne umożliwiające świadczenie usługi chmurowej.

„Personel", w tym personel zarządzany przez podwykonawców, oznacza osoby, które obsługują świadczenie usługi będącej przedmiotem audytu i zarządzają taką usługą oraz czuwają nad jej bezpieczeństwem, dostępnością lub działaniem.

3. Kryterium audytu C – Usytuowanie danych w Unii

Organizacja audytowa powinna ocenić kryterium audytu wymienione w załączniku II, lit. c) dla unijnych poziomów uzasadnienia zaufania 2, 3 i 4 w oparciu o następujące ustalenia:

1) Dowody potwierdzające, że dane klientów są przechowywane i przetwarzane wyłącznie w Unii oraz że osoby trzecie lub podwykonawcy, którzy nie spełniają warunków określonych w niniejszym załączniku, w żadnym wypadku nie są w stanie – ani pod względem technicznym, ani operacyjnym – uzyskać dostępu do danych klientów, a także pozyskać, udostępnić, zniszczyć ani, w ogólniejszym ujęciu, przetwarzać takich danych bez uprzedniej zgody. Przykłady takich dowodów obejmują rejestry dostępu, zasady dostępu do wsparcia technicznego, rejestry uprzywilejowanego dostępu, politykę przechowywania kopii zapasowych, schemat przepływu danych wskazujący, gdzie dane klientów są przechowywane, przetwarzane, powielane i archiwizowane. W przypadku przetwarzania danych osobowych – umowy z podwykonawcami potwierdzające zgodność z rozporządzeniem (UE) 2016/679.

2) Dowody w postaci rejestrów i zapisów z monitorowania potwierdzające, że wszystkie dane są przechowywane i przetwarzane wyłącznie w Unii. Przykłady obejmują umowy ramowe o świadczenie usług, umowy o przetwarzaniu danych,

umowy dotyczące rezydencji danych lub wszelkie ograniczenia dotyczące przepływu danych w UE.

3) Dowody (takie jak umowy, rejestry i procedury przedstawione organom sektora publicznego) potwierdzające, że audytowany dostawca i podwykonawcy zaangażowani w świadczenie usługi będącej przedmiotem audytu wprowadzili niezbędne środki gwarantujące, że:

   a) żadne dane klientów, w tym dane zaszyfrowane, nie są przekazywane poza Unię bez zgody organu sektora publicznego;

   b) żadne dane nie są przekazywane osobom trzecim innym niż podwykonawcy zaangażowani w świadczenie usługi lub odbiorcy wyraźnie upoważnieni przez organ sektora publicznego.

4) Schemat przepływu danych przedstawiający przepływy danych między dostawcą usług chmurowych a danymi klientów, z uwzględnieniem usług osób trzecich i podwykonawców. Na schemacie należy wyraźnie określić źródło i przeznaczenie danych oraz wykazać, że dane nie opuszczają Unii.

UWAGA: do celów niniejszego załącznika „klient" oznacza organ sektora publicznego, który zawarł umowę lub inne prawnie wiążące porozumienie z dostawcą usług chmurowych w celu uzyskania dostępu do usługi chmurowej lub korzystania z takiej usługi.

„Dane klientów" mogą oznaczać wszelkie dane pozostające pod kontrolą klienta korzystającego z usługi chmurowej – czy to na mocy przepisów prawa, umowy, czy też na innej podstawie – które są:

   a) wprowadzane do usługi chmurowej przez klienta lub w jego imieniu, w tym dane uwierzytelniające;

   b) generowane w wyniku korzystania przez klienta z usługi chmurowej.

Dane klientów mogą również obejmować dane pozostające pod kontrolą audytowanych dostawców, które pozyskano w wyniku interakcji klienta korzystającego z usługi chmurowej z usługą będącą przedmiotem audytu. Obejmuje to dane klientów i wszelkie dane wynikające z korzystania z usług chmurowych (tj. dane telemetryczne, metadane).

„Dane pozyskane z usługi chmurowej" obejmują tę część zarejestrowanych danych, która zawiera zapisy dotyczące tego, kto korzystał z usługi, kiedy miało to miejsce, z jakich funkcji korzystano, jakiego rodzaju danych to dotyczyło itp. Dane te mogą również obejmować informacje o liczbie uprawnionych użytkowników oraz ich tożsamości. Mogą to być również wszelkie dane dotyczące konfiguracji lub personalizacji, o ile w usłudze chmurowej przewidziano możliwość jej konfiguracji i personalizacji.

4. Kryterium audytu D – Obywatelstwo Unii

Organizacja audytowa powinna ocenić kryterium audytu wymienione w załączniku II, lit. d) dla unijnych poziomów uzasadnienia zaufania 2, 3 i 4 w oparciu o następujące ustalenia:

1) audytowany dostawca powinien przedstawić organizacji audytowej dowody potwierdzające, że wdrożył środki mające na celu zapewnienie, aby pracownicy zaangażowani w świadczenie usługi będącej przedmiotem audytu mogli na żądanie organu sektora publicznego wykazać, że są obywatelami Unii. Na potwierdzenie można przedstawić ważne dokumenty urzędowe wydane przez organy rządowe (np. ważny paszport i krajowy dowód tożsamości);

2) audytowany dostawca powinien przedstawić schematy organizacyjne i opisy stanowisk potwierdzające, że na stosowne żądanie jest w stanie zapewnić, aby dostęp do obsługi, konserwacji i wsparcia usługi będącej przedmiotem audytu oraz zarządzania taką usługą mieli wyłącznie pracownicy posiadający obywatelstwo unijne;

3) audytowany dostawca powinien przedstawić dokumenty potwierdzające zasady kontroli dostępu oraz ścieżki audytu, z których wynika, że dostęp do systemów i danych usługi mają wyłącznie upoważnieni pracownicy będący obywatelami Unii;

4) audytowany dostawca powinien wykazać, że wprowadził procedury opisujące sposób weryfikacji obywatelstwa przed zaangażowaniem pracownika w świadczenie usługi oraz sposób zapewnienia zgodności z tym kryterium audytu przez cały okres zatrudnienia.

UWAGA: *do personelu zaangażowanego w świadczenie usługi będącej przedmiotem audytu mogą należeć osoby posiadające dostęp logiczny lub fizyczny do infrastruktury i aktywów wykorzystywanych do obsługi usługi chmurowej, a także osoby odpowiedzialne za obsługę klienta oraz cały personel sprawujący kontrolę zarządczą nad dostawcą usług chmurowych.*

5. Kryteria audytu E – Europejski program certyfikacji cyberbezpieczeństwa przyjęty na podstawie rozporządzenia 2019/881

Organizacja audytowa powinna ocenić kryterium audytu wymienione w załączniku II, lit. e) dla unijnych poziomów uzasadnienia zaufania 2, 3 i 4 w oparciu o następujące ustalenia:

1) ważny europejski certyfikat cyberbezpieczeństwa wydany przez właściwą jednostkę oceniającą zgodność, potwierdzający, że usługę będącą przedmiotem audytu oceniono i uznano za zgodną z wymogami odpowiadającymi „podstawowemu", „istotnemu" lub „wysokiemu" poziomowi uzasadnienia zaufania w ramach europejskiego programu certyfikacji cyberbezpieczeństwa przyjętego na podstawie rozporządzenia (UE) 2019/881, pod warunkiem, że taki program został ustanowiony;

2) sprawozdanie certyfikacyjne zawierające opis głównych komponentów wykorzystywanych do opracowania i korzystania z usługi chmurowej, która jest objęta świadectwem audytu;

3) do czasu ustanowienia europejskiego programu certyfikacji cyberbezpieczeństwa obejmującego usługi chmurowe audytowany dostawca może wykazać zgodność z przepisami, przedstawiając ważne certyfikaty cyberbezpieczeństwa. Mogą one obejmować między innymi:

   a) ważny certyfikat wydany przez właściwą jednostkę oceniającą zgodność (zgodnie ze specyfikacjami technicznymi CEN/CLC/TS 18072:2025) potwierdzający, że usługa chmurowa została oceniona i uznana za zgodną z wymogami odpowiadającymi „podstawowemu", „istotnemu" lub „wysokiemu" poziomowi uzasadnienia zaufania, które zdefiniowano w specyfikacjach technicznych CEN/TS 18026:2024;

   b) ważny certyfikat wydany przez odpowiedni właściwy organ krajowy, potwierdzający, że usługa chmurowa została oceniona i uznana za zgodną z wymogami w ramach krajowego programu cyberbezpieczeństwa obowiązującego obecnie w danym państwie członkowskim;

   c) w przypadku braku programu krajowego – dowody potwierdzające przestrzeganie najwyższych norm cyberbezpieczeństwa dostępnych na rynku.

6. Kryterium audytu F – Systemy AI obsługiwane przez państwo trzecie lub podmiot prawny z państwa trzeciego

Organizacja audytowa powinna ocenić kryterium audytu wymienione w załączniku II, lit. f) dla unijnych poziomów uzasadnienia zaufania 2, 3 i 4 w oparciu o następujące ustalenia:

1) Klauzule umowne stanowiące, że dane przetwarzane lub generowane w ramach korzystania z usługi będącej przedmiotem audytu, w tym dane pozyskane od klienta, rejestry zdarzeń i dane telemetryczne, nie będą wykorzystywane do trenowania ani dostrajania żadnego modelu lub systemu AI obsługiwanego przez państwo trzecie lub podmiot prawny z państwa trzeciego i w żadnym wypadku nie będą przekazywane poza Unię.

2) Klauzule umowne określające, że dane są przetwarzane wyłącznie w celu świadczenia usługi będącej przedmiotem audytu, a nie w celu ulepszenia usługi, modelu lub systemu lub w jakimkolwiek innym celu wtórnym.

3) Schematy przepływu danych dokumentujące pełny przepływ danych, obejmujący przyjmowanie, przechowywanie, przetwarzanie i usuwanie danych. Na schematach należy również wskazać, w których miejscach potoki AI lub operacje uczenia maszynowego (MLOps) łączą się z danymi klientów.

4) Dokumentacja MLOps lub dokumentacja wdrożeniowa potwierdzająca, że operacje tworzenia, testowania i wdrażania ma miejsce na terytorium UE.

5) Karty modeli lub systemów zawierające nazwę modelu lub systemu, wersję, źródła danych treningowych i walidacyjnych, w tym oświadczenia, że dane wygenerowane w wyniku korzystania z usługi będącej przedmiotem audytu nie opuszczają terytorium Unii.

6) Polityki dotyczące pochodzenia danych i powiązane dokumenty wdrożeniowe, z których wynika, że dostawca korzysta z narzędzi do śledzenia pochodzenia danych i trasy ich przepływu oraz że może wykazać (w odniesieniu do każdego wpisu), w jakim celu dane zostały wykorzystane.

7) Wykaz podwykonawców (ze wskazaniem kraju, w którym mają oni siedzibę), którzy mają dostęp do danych wygenerowanych w wyniku korzystania z usługi będącej przedmiotem audytu.

7. Kryterium audytu G – Brak kontroli ze strony państwa trzeciego lub kontroli ze strony jednostki z państwa trzeciego

Organizacja audytowa powinna ocenić kryterium audytu wymienione w załączniku II, lit. g) dla unijnych poziomów uzasadnienia zaufania 2, 3 i 4 w oparciu o następujące ustalenia:

1) Organizacja audytowa powinna określić i przeanalizować:

   a) wszystkich bezpośrednich i pośrednich udziałowców, aż do ostatecznych właścicieli;

   b) tabelę kapitalizacji dokumentującą strukturę własności spółki;

   c) organ lub organy uprawnione do podejmowania strategicznych decyzji (walne zgromadzenie wspólników, rada nadzorcza, zarząd itp.);

   d) zasady powoływania, wyboru i odwoływania organów zarządzających oraz faktyczny skład organów zarządzających (np. w celu ustalenia, czy którykolwiek udziałowiec jest uprawniony do wyznaczenia przedstawiciela zarządu lub dysponuje większością miejsc w zarządzie);

e) kworum i większość wymagane do podejmowania decyzji strategicznych, w celu ustalenia, czy którykolwiek udziałowiec może podjąć decyzję strategiczną (czy to dlatego, że dysponuje wymaganą większością do zatwierdzenia takiej decyzji, czy też dlatego, że może zablokować taką decyzję, korzystając z prawa weta lub innych szczególnych uprawnień, nawet jeśli nie może samodzielnie narzucić takiej decyzji itp.);

f) ewentualny wpływ na decyzje strategiczne poprzez powiązania handlowe, finansowe lub inne środki itp.

2) Audytowany dostawca powinien zwrócić się do swoich podwykonawców o udzielenie wszystkich powyższych informacji i udostępnić je organizacji audytowej.

7.1. Ocena własności i kontroli:

1) Audytowany dostawca powinien przedstawić organizacji audytowej następujące dowody dotyczące siedziby głównej:

a) lokalizację i pełny adres globalnej siedziby głównej lub siedziby zarządu;

b) lokalizacje zarządczych struktur wykonawczych.

2) Audytowany dostawca powinien przedstawić organizacji audytowej następujące dowody dotyczące struktury własności i szczególnych praw:

a) Szczegółowy wykaz zawierający informacje o wszystkich właścicielach, którzy:

i. posiadają, bezpośrednio lub pośrednio, co najmniej 5 % kapitału lub co najmniej 5 % praw głosu, w tym na mocy jakiegokolwiek porozumienia, umowy, powiązania lub poprzez pośredników. Obejmuje to porozumienia w sprawie głosowania między udziałowcami, którzy łącznie dysponowaliby ponad 5 % praw głosu lub 5 % kapitału;

ii. posiadają co najmniej jedno z następujących szczególnych praw związanych z posiadaniem udziałów: a) prawo weta wobec przeniesienia udziałów; b) prawo pierwokupu; c) prawo do nabycia dodatkowych udziałów lub inwestycji na określonych warunkach.

b) Organizacja audytowa powinna zażądać następujących dokumentów potwierdzających w celu oceny elementów, o których mowa w ust. 2 lit. a):

i. wyciągi z rejestru handlowego i księgi rachunkowe udziałowców organizacji oraz wszelkie inne istotne dokumenty, w których wyraźnie wskazano udziałowców i ich prawa głosu lub procentowy udział w kapitale;

ii. umowa wspólników, protokół ustaleń między udziałowcami, statut, umowa spółki lub inne istotne dokumenty dotyczące procedur podejmowania decyzji w ramach podmiotu prawnego, umowy inwestycyjne między udziałowcami itp.;

iii. w przypadku udziałowców będących osobami prawnymi, którzy posiadają co najmniej 5 % kapitału lub co najmniej 5 % praw głosu:

1) wykres przedstawiający poszczególne poziomy własności lub łańcuch kontroli aż do ostatecznych właścicieli;

2) umowa spółki, regulamin lub równoważne dokumenty założycielskie;

3) rejestr członków zarządu, kadry kierowniczej i osób uprawnionych do podpisywania dokumentów.

3) Audytowany dostawca powinien przedstawić organizacji audytowej następujące dowody dotyczące ładu korporacyjnego:

a) Audytowany dostawca powinien przedstawić organizacji audytowej opis:

i. organów decyzyjnych, ich składu oraz obywatelstwa lub miejsca prowadzenia działalności przez ich członków (w stosownych przypadkach);

ii. zasad dotyczących wyboru, mianowania, powoływania lub kadencji członków organów decyzyjnych lub osób zajmujących inne stanowiska kierownicze;

iii. procedur podejmowania decyzji, w tym informacji na temat wymaganej większości lub kworum niezbędnego do podjęcia decyzji;

iv. zasad zarządzania wewnętrznego opisujących sposób rejestrowania i zatwierdzania decyzji dotyczących własności i kontroli;

decyzji zarządu i kierownictwa odzwierciedlających określoną strukturę kontroli;

protokołów posiedzeń zarządu i uchwał dotyczących zmian kontrolnych.

b) Audytowany dostawca powinien przedstawić organizacji audytowej dokumenty potwierdzające, określające lub opisujące: organy decyzyjne i zasady dotyczące ich wyboru, powoływania, mianowania lub kadencji, procedury decyzyjne, prawa głosu, prawa weta, prawa do mianowania oraz prawa do zatwierdzania w ramach podmiotu prawnego (np. umowy spółki, statuty, sprawozdania dotyczące ładu korporacyjnego itp.). Dokumenty i informacje potwierdzające należy przedstawić w odniesieniu do każdego podmiotu prawnego niższego szczebla, który bezpośrednio lub pośrednio posiada co najmniej 5 % kapitału lub praw głosu, aż do ostatecznych właścicieli wszystkich zaangażowanych szczebli.

4) Audytowany dostawca powinien przedstawić organizacji audytowej następujące dowody dotyczące kontroli:

a) Audytowany dostawca powinien przedstawić organizacji audytowej dowody potwierdzające istnienie powiązań handlowych, które dają możliwość sprawowania kontroli. Obejmuje to między innymi wykaz osób fizycznych lub prawnych, z którymi audytowani dostawcy (lub właściciele audytowanego dostawcy, w tym podmioty niższego szczebla aż do ostatecznych właścicieli) utrzymują stosunki handlowe, które a) dają możliwość sprawowania podobnego poziomu kontroli nad zarządzaniem i zasobami, jak posiadanie udziałów lub aktywów; oraz b) mają charakter długookresowy (np. bardzo istotne długoterminowe umowy na dostawy lub kredyty udzielane przez producentów oprogramowania lub klientów w połączeniu z powiązaniami strukturalnymi).

b) Dokumenty potwierdzające powinny obejmować umowy o współpracy z organami sektora publicznego lub producentami oprogramowania itp.

5) Audytowany dostawca powinien przedstawić organizacji audytowej następujące dowody dotyczące powiązań finansowych dających możliwość sprawowania kontroli:

a) Audytowany dostawca powinien sporządzić wykaz osób fizycznych lub prawnych (w tym udziałowców lub właścicieli posiadających pakiet kontrolny), od których audytowany dostawca lub jego właściciele są finansowo zależni w sposób, który mógłby umożliwić im uzyskanie przywilejów w strategicznych obszarach działalności.

b) Dokumenty potwierdzające powinny obejmować dokumenty kredytowe, regulaminy oraz dokumenty potwierdzające powiązania finansowe itd.

6) Audytowany dostawca powinien przedstawić organizacji audytowej następujące dowody dotyczące innych źródeł sprawowania kontroli:

a) audytowani dostawcy powinni poinformować organizację audytową, czy istnieją jakiekolwiek inne środki, procesy lub powiązania, w ramach których przyznaje się kontrolę innemu państwu trzeciemu lub podmiotowi prawnemu mającemu siedzibę w państwie trzecim (które dają możliwość sprawowania podobnego poziomu kontroli nad zarządzaniem i zasobami, jaki wynikałby z posiadania udziałów lub aktywów, oraz mają charakter długookresowy).

b) Dokumenty potwierdzające powinny zawierać dowody na potwierdzenie takiej kontroli lub oświadczenie o jej braku (może to być oświadczenie zarządu dostawcy usług).

UWAGA: *przy ocenie kontroli należy wziąć pod uwagę takie elementy jak struktury własności i szczególne prawa, ład korporacyjny, powiązania handlowe przyznające kontrolę, powiązania finansowe przyznające kontrolę oraz wszelkie inne źródła kontroli.*

7.2. Dodatkowe działania wynikające z oceny własności i kontroli

Jeżeli organizacja audytowa stwierdzi, że audytowany dostawca podlega kontroli państwa trzeciego lub podmiotu prawnego z państwa trzeciego, powinna zażądać przedstawienia następujących dodatkowych dowodów:

c) potwierdzenie, że Komisja podjęła decyzję na podstawie art. 19 w odniesieniu do państwa trzeciego, pod kontrolą którego znajduje się dostawca usług chmurowych;

d) wszelkie dowody potwierdzające, że audytowany dostawca i każdy podwykonawca zaangażowany w świadczenie usługi będącej przedmiotem audytu wdrożyli niezbędne środki w celu wyegzekwowania skutecznego rozdzielenia prawnego, technicznego i organizacyjnego między dostawcą usług chmurowych a jakimkolwiek państwem trzecim lub podmiotem prawnym mającym siedzibę w państwie trzecim, gwarantujące, że dostawca usług chmurowych nie jest w stanie spełnić, pod względem prawnym, technicznym i operacyjnym, żadnego żądania udzielenia dostępu do danych klientów, w tym zaszyfrowanych danych, ani żadnego żądania dotyczącego zakłócenia ciągłości usług lub obniżenia ich jakości;

e) wszelkie dowody potwierdzające, że organ sektora publicznego zostanie poinformowany o każdym takim żądaniu oraz uzyska potwierdzenie, że żądanie to zostało odrzucone;

f) wszelkie dowody potwierdzające prowadzenie aktualnego rejestru wszelkich wniosków skierowanych przez państwo trzecie lub podmiot prawny z siedzibą w państwie trzecim w sprawie dostępu do danych klientów, zakłócenia ciągłości świadczenia usług lub obniżenia jakości usług, zawierające co najmniej treść wniosku oraz odpowiedź na ten wniosek.

8. Kryterium audytu H – Brak korzystania ze wsparcia technicznego i operacyjnego poza Unią

Organizacja audytowa powinna ocenić kryterium audytu wymienione w załączniku II, lit. h) dla unijnych poziomów uzasadnienia zaufania 2, 3 i 4 w oparciu o następujące ustalenia:

1) dowody potwierdzające, że audytowany dostawca wdrożył wiążące klauzule umowne stanowiące, że wszelkie działania w zakresie wsparcia, administracji, utrzymania, monitorowania, reagowania na incydenty i działania operacyjne muszą być inicjowane i prowadzone wyłącznie na terenie Unii. Mogą to być na przykład klauzule umowne wymagające uprzedniego ujawnienia informacji o wszystkich podwykonawcach i lokalizacjach wsparcia, uzyskania uprzedniej pisemnej zgody przed zaangażowaniem nowych podwykonawców oraz ustanawiające prawo do odrzucenia wszelkich podwykonawców zlokalizowanych poza Unią;

2) dowody potwierdzające, że audytowany dostawca prowadzi aktualny rejestr podwykonawców;

3) dowody potwierdzające, że audytowany dostawca nie powierza takich działań podwykonawcom spoza Unii ani nie przenosi takich działań poza Unię;

4) dowody potwierdzające, że audytowany dostawca wdrożył niezbędne środki prawne, techniczne i organizacyjne w celu wykluczenia możliwości uzyskania zdalnego dostępu do wsparcia technicznego i operacyjnego spoza Unii na potrzeby usługi będącej przedmiotem audytu;

5) dowody potwierdzające, że usługi pomocy technicznej lub wsparcia świadczone przez audytowanego dostawcę, zarządzanie infrastrukturą, działalność centrum operacji bezpieczeństwa (SOC) lub centrum operacji sieciowych (NOC) takiego dostawcy, dostęp uprzywilejowany, obsługa kopii zapasowych i operacje przywracania gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej w odniesieniu do usługi będącej przedmiotem audytu są świadczone wyłącznie z terytorium Unii, w tym ścieżka dostępu niezbędna do obsługi usługi;

6) dowody potwierdzające, że audytowany dostawca zapewnia, aby personel po odejściu z przedsiębiorstwa nie miał dalszego dostępu do usługi będącej przedmiotem audytu, oraz cofa wszystkie uprawnienia dostępu;

7) dowody potwierdzające, że audytowany dostawca wdrożył niezbędne środki techniczne i organizacyjne w celu zapewnienia, aby dostęp administracyjny do systemów wykorzystywanych do obsługi usługi będącej przedmiotem audytu odbywał się za pośrednictwem ścieżek dostępu znajdujących się na terytorium Unii. Można to wykazać poprzez wdrożenie ograniczonych geograficznie kontroli sieci, unijnej infrastruktury administracyjnej, środków kontroli uprzywilejowanego dostępu oraz mechanizmów monitorowania;

8) dowody potwierdzające, że audytowany dostawca dysponuje procedurami wykluczającymi sprawowanie skutecznej kontroli przez państwo trzecie lub podmiot prawny z siedzibą w państwie trzecim, również w przypadku podzlecenia na zasadzie outsourcingu.

9. Kryterium audytu I – Zapewnienie przejrzystości łańcucha dostaw oprogramowania

Organizacja audytowa powinna ocenić kryterium audytu wymienione w załączniku II, lit. i) dla unijnych poziomów uzasadnienia zaufania 2, 3 i 4 w oparciu o następujące ustalenia:

1) Audytowany dostawca powinien udostępnić organizacji audytowej kompletne i aktualne zestawienie podstawowych materiałów do produkcji oprogramowania (SBOM) w odniesieniu do wszystkich komponentów oprogramowania, w tym otwartego oprogramowania (OSS).

2) Audytowany dostawca powinien udostępnić organizacji audytowej wykaz zależności. Wykaz ten powinien zawierać:

   a) wszystkie wykorzystywane moduły oprogramowania, biblioteki lub interfejsy programowania aplikacji (API), a także narzędzia programistyczne;

   b) informacje o pochodzeniu oprogramowania: informacje o tym, gdzie (kraj pochodzenia) i przez kogo oprogramowanie zostało zaprojektowane i opracowane oraz gdzie i przez kogo jest utrzymywane, a także o miejscu dystrybucji oprogramowania oraz jurysdykcji, której podlega takie oprogramowanie, oraz jego aktualizacjach;

   c) stopień zależności od dostawców, zakładów lub zamkniętych technologii spoza UE; w przypadku poziomu 3 – dowody potwierdzające, że w przypadku gdy stos oprogramowania jest dostarczany przez podmiot z kraju trzeciego, nie obowiązują żadne nieuzasadnione ograniczenia licencyjne;

   d) stopień zależności od oprogramowania otwartego;

   e) wgląd w cały łańcuch producentów i podwykonawców oprogramowania, w tym prawa do prowadzania audytów.

***Uwaga**: powyższe wymogi oznaczają, że spółki joint venture utworzone np. przez podmiot unijny z podmiotem prawnym mającym siedzibę w państwie trzecim mogą kwalifikować się do tego poziomu.*

3) Audytowany dostawca powinien przedstawić:

   a) dowody potwierdzające istnienie opartego na analizie ryzyka procesu identyfikacji i ograniczania zależności od zewnętrznych producentów oprogramowania, które to zależności mają znaczenie dla funkcjonowania usługi chmurowej;

   b) dowody potwierdzające, że dostawca zidentyfikował co najmniej jedno alternatywne rozwiązanie w zakresie oprogramowania, w tym otwarte oprogramowanie. Jeżeli nie można zidentyfikować równoważnego oprogramowania, należy wskazać rozwiązanie zapewniające minimalną funkcjonalność. Należy przeprowadzić testy i plan przełączenia umożliwiający migrację do takich alternatywnych rozwiązań;

   c) dowody potwierdzające możliwość migracji do alternatywnego rozwiązania w przypadku wystąpienia jakiejkolwiek usterki lub awarii u dostawcy lub w przypadku wprowadzenia ograniczeń przez państwo trzecie lub podmiot prawny mający siedzibę w państwie trzecim;

d) wykaz otwartych standardów, których audytowany dostawca przestrzega w ramach swojej polityki w odniesieniu do usługi będącej przedmiotem audytu.

4) Audytowany dostawca powinien zapewnić przejrzystość poprzez zdalny dostęp i możliwość kontroli kodu źródłowego:

a) udostępniając organizacji audytowej wykaz dowodów potwierdzających, że nie zastosowano żadnych zdalnych funkcji ani mechanizmów, które mogłyby zostać wykorzystane do istotnej ingerencji w urządzenie, system lub oprogramowanie lub do zakłócenia ich działania. Wykaz ten powinien zawierać:

i. dowody potwierdzające, że przetestowano komponent oprogramowania, aby zapobiec wykorzystywaniu jakichkolwiek zdalnych funkcji lub mechanizmów, które mogłyby posłużyć do istotnej ingerencji w urządzenie, system lub oprogramowanie lub do zakłócenia ich działania (procedura testowa, sprawozdania z testów, plan testów itp.);

ii. dowody potwierdzające, że stosowane przez organizację procedury zarządzania zmianami obejmują wszelkie zmiany w oprogramowaniu układowym, BIOS i aktualizacjach oprogramowania, a także integrację nowych komponentów, które mają zapobiec wykorzystaniu jakichkolwiek funkcji lub mechanizmów zdalnych;

iii. dowody potwierdzające, że procedura konserwacji jest aktualizowana i że uwzględnia się w niej wszelkie zdalne funkcje lub mechanizmy, które mogłyby zostać wykorzystane do istotnej ingerencji w urządzenie, system lub oprogramowanie lub do zakłócenia ich działania.

b) Audytowany dostawca musi zapewnić niezależnemu audytorowi będącemu osobą trzecią prawo dostępu do kodu źródłowego takiego oprogramowania i możliwość kontroli tego kodu. Audytowany dostawca musi również zapewnić, aby całość dokumentacji, materiałów technicznych i informacji niezbędnych do oceny i audytu kodu źródłowego zostały udostępnione organizacji audytowej w kompletnym, dokładnym i przystępnym formacie.

10. Kryterium audytu J – Otwarte oprogramowanie

Organizacja audytowa powinna ocenić kryterium audytu wymienione w załączniku II, lit. j) dla unijnych poziomów uzasadnienia zaufania 2, 3 i 4 w oparciu o następujące ustalenia:

1) Audytowany dostawca powinien zapewnić przejrzystość poprzez zdalny dostęp i możliwość kontroli kodu źródłowego:

a) udostępniając organizacji audytowej wykaz dowodów potwierdzających, że nie zastosowano żadnych zdalnych funkcji ani mechanizmów, które mogłyby zostać wykorzystane do istotnej ingerencji w urządzenie, system lub oprogramowanie lub do zakłócenia ich działania. Wykaz ten powinien zawierać:

i. dowody potwierdzające, że przetestowano komponent oprogramowania, aby zapobiec wykorzystywaniu jakichkolwiek zdalnych funkcji lub mechanizmów, które mogłyby posłużyć do istotnej ingerencji w urządzenie, system lub oprogramowanie lub do

zakłócenia ich działania (procedura testowa, sprawozdania z testów, plan testów itp.);

ii. dowody potwierdzające, że stosowane przez organizację procedury zarządzania zmianami obejmują wszelkie zmiany w oprogramowaniu układowym, BIOS i aktualizacjach oprogramowania, a także integrację nowych komponentów, które mają zapobiec wykorzystaniu jakichkolwiek funkcji lub mechanizmów zdalnych;

iii. dowody potwierdzające, że procedura konserwacji jest aktualizowana i że uwzględnia się w niej wszelkie zdalne funkcje lub mechanizmy, które mogłyby zostać wykorzystane do istotnej ingerencji w urządzenie, system lub oprogramowanie lub do zakłócenia ich działania.

2) Audytowany dostawca powinien przedstawić:

a) dowody przeprowadzenia procesu opartego na analizie ryzyka, mającego na celu identyfikację i ograniczenie ryzyka: (i) niedostatecznego wsparcia ze strony ekosystemu i społeczności w ramach otwartego oprogramowania; (ii) braku stałego monitorowania publikowanych aktualizacji; (iii) przypadków, w których otwarte oprogramowanie jest przestarzałe lub nie jest już utrzymywane;

b) dowody potwierdzające, że audytowany dostawca bez zbędnej zwłoki wdrożył aktualne otwarte oprogramowanie;

c) dowody potwierdzające, że audytowany dostawca zidentyfikował co najmniej jedno alternatywne rozwiązanie oparte na otwartym oprogramowaniu. Jeżeli audytowany dostawca nie jest w stanie zidentyfikować równoważnego oprogramowania, musi znaleźć rozwiązanie zapewniające minimalną możliwą funkcjonalność. Audytowany dostawca musi wdrożyć testy i plan przełączenia umożliwiający migrację do rozwiązań alternatywnych.

3) W przypadku gdy audytowany dostawca korzysta z oprogramowania udostępnionego na podstawie licencji otwartego oprogramowania, dostawca ten powinien wdrożyć mechanizmy umożliwiające wykrycie sytuacji, w której oprogramowanie to zostanie nabyte przez państwo trzecie lub podmiot prawny lub fundację z siedzibą w państwie trzecim, lub znajdzie się pod ich kontrolą, oraz niezwłoczne powiadomienie o tym organu sektora publicznego.

11. Kryterium audytu K – Usługi globalne i jednostki zależne w państwach trzecich

Organizacja audytowa powinna ocenić kryterium audytu wymienione w załączniku II, lit. k) dla unijnych poziomów uzasadnienia zaufania 2, 3 i 4 w oparciu o następujące ustalenia:

1) Organizacja audytowa powinna sprawdzić, czy jednostka zależna jest prawnie i operacyjnie niezależna od audytowanego dostawcy.

2) Audytowany dostawca musi wykazać, że jednostka zależna nie ma dostępu do systemów przetwarzających lub przechowujących dane klientów.

3) Audytowany dostawca musi wykazać, że jednostka zależna nie posiada kont uprzywilejowanych w unijnych środowiskach produkcyjnych, w tym żadnych uprawnień do administrowania chmurą, zarządzania tożsamością i dostępem (IAM), zarządzania dostępem uprzywilejowanym (PAM), ani monitorowania baz danych i administrowania bazami danych.

4) Organizacja audytowa powinna sprawdzić, czy personel jednostki zależnej nie może uzyskać dostępu do danych klientów w Unii.

5) Organizacja audytowa powinna sprawdzić, czy jednostka zależna nie ma uprawnień do wydawania pracownikom operacyjnym w Unii żadnych poleceń dotyczących ujawniania danych klientów lub omijania procedur bezpieczeństwa.

6) Organizacja audytowa powinna sprawdzić, czy wszystkie skierowane do jednostki zależnej wnioski rządów innych państw są formalnie przekierowywane do właściwego podmiotu Unii w celu przeprowadzenia ich oceny prawnej zgodnie z prawem Unii i państwa członkowskiego.