LEWIATAN

Warszawa, 18 października 2023 r.
KL/397/182/AM/2023

Pan
Janusz Cieszyński
Pełnomocnik Rządu ds. Cyberbezpieczeństwa
Minister Cyfryzacji

Szanowny Panie Ministrze,

Kontynuując konstruktywny dialog z Ministerstwem Cyfryzacji w sprawie prac nad zmianami w WIIP, tj. w projekcie uchwały Rady Ministrów zmieniającej uchwałę nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa", Konfederacja Lewiatan, w załączeniu, przesyła propozycje uwag do nowej wersji projektu.
Jednocześnie chcemy bardzo podziękować za wszystkie pozytywne zmiany wprowadzone do tekstu projektu.

Z poważaniem

Maciej Witucki
Prezydent Konfederacji Lewiatan

Do wiadomości:
Pan Łukasz Wojewoda – Dyrektor Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji
Pani Katarzyna Bis-Płaza – Dyrektorka Departamentu Projektów i Strategii, Ministerstwo Cyfryzacji

Załącznik: Stanowisko KL do projektu uchwały Rady Ministrów zmieniającej uchwałę nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (wersja projekty z dnia 29 września br.)

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

Stanowisko KL do projektu uchwały Rady Ministrów zmieniającej uchwałę nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (wersja projekty z dnia 29 września br.)

I. Uwagi ogólne

Konfederacja Lewiatan na wstępnie chce podziękować za wszystkie pozytywne zmiany wprowadzone do tekstu projektu uchwały w jej najnowszej wersji, tj:

1. **Par. 3a p. 5 – został usunięty z obecnej wersji projektu uchwały:**

   „5. Nieuwzględnienie rekomendacji stanowi podstawę do wystąpienia przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa do organu sprawującego nadzór nad podmiotami, o których mowa w § 6 ust. 1, z informacją o ich nieuwzględnieniu."

2. **Par. 6 ust. 3 – przeniesienie deklaracji zgodności z potencjalnego użytkownika na dostawcę**
   Dzięki temu zapisowi dostawca usług stworzy raz deklarację, zamiast tworzył oddzielnie deklaracji przez podmiot-użytkownika.

3. **Par. 8 – zmiana z obowiązku wnioskowania na możliwość wnioskowania**
   Obowiązująca wersja projektu uchwały

   *„8. Podmioty, o których mowa w § 6 ust. 1, w celu skorzystania z usług przetwarzania w publicznych chmurach obli[1]czeniowych **wnioskują**…"*
   *Propozycja: „8. Podmioty, o których mowa w § 6 ust. 1, przed przystąpieniem do korzystania z usług przetwarzania w publicznych chmurach obliczeniowych **mogą wystąpić z wnioskiem**…"*

Poniżej przedstawiamy dodatkowe uwagi do obecnej wersji projektu uchwały:

Lewiatan z zadowoleniem przyjmuje inicjatywę nowelizacji projektu Uchwały Rady Ministrów z 2019 roku ((projekt z dnia 28.09. 2023 roku)) która, na skutek upływu czasu i postępu w rozwoju technologii , zdezaktualizowała się w znacznym stopniu i nie odpowiada potrzebom administracji publicznej ani ofercie rynku usług chmurowych .
Warto przypomnieć zakres inicjatywy która stała u podstaw przyjęcia w/w uchwały w 2019 roku (https://www.gov.pl/web/cyfryzacja/wspolna-infrastruktura-panstwa-wip-20,:

Zakres Inicjatywy WIIP

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

Program WIIP odpowiada za podniesienie bezpieczeństwa danych przetwarzanych w systemach teleinformatycznych podmiotów administracji publicznej oraz optymalizacji kosztów utrzymania tych systemów. Wprowadzenie jednolitych, wysokich standardów ochrony systemów informatycznych i wspieranie podmiotów administracji publicznej w utrzymaniu tych systemów oraz uzyskiwaniu usług niezbędnych do ich budowy, rozwoju i utrzymania przyczyni się do zapewnienia wysokiego poziomu usług świadczonych społeczeństwu przez administrację publiczną. Program WIIP zakłada optymalizację istniejących zasobów teleinformatycznych i aplikacji w administracji publicznej poprzez dostarczanie nowoczesnych i optymalnych kosztowo technologii informatycznych. Taki sposób funkcjonowania administracji publicznej pozwoli na ustalenie priorytetów w podnoszeniu poziomu bezpieczeństwa, kompleksowych planów migracji, a także zrównoważeniu wykorzystania rozwiązań chmurowych.

Wg pierwotnego założenia Uchwała Rady Ministrów z 24 września 2019 roku była rezultatem analiz posiadanych zasobów infrastruktury informatycznej administracji przeprowadzonej siłami Ministerstwa Cyfryzacji. Analiza wskazywała na wykorzystywanie ogromnej liczby rozproszonych (kilkuset) serwerowni (CPD), trudnościach w zapewnieniu jakości usług, SLA, cyberbezpieczeństwa, procedur czy kwalifikacji personelu. Ważnym aspektem były wysokie koszty oprogramowania wynikające m.in. z braku możliwości dokonywania jednolitych zakupów w dużej skali czy przenoszenia licencji pomiędzy podmiotami. Celem inicjatywy było optymalizacja wykorzystania potencjału infrastruktury, uzyskanie większej elastyczności, zmniejszenie kosztów i podniesienie odporności i poziomu cyberbezpieczeństwa. Chmura obliczeniowa, zarówno Rządowa Chmura Obliczeniowa, jak i publiczne chmury obliczeniowe lub ich hybrydowe formy powinny stać się formą osiągnięcia tych celów.

Zgadzamy się absolutnie ze stanowiskiem, że Państwo może tworzyć szczególne i własne wymagania dot. regulacji w zakresie cyberbezpieczeństwa i przetwarzania danych w jednostkach podległych Radzie Ministrów w oparciu o jasne i przejrzyste reguły. Zdecydowanie popieramy tez nowatorskie poszukiwania rozwiązań w których z jednej strony powstaje wspólnotowe środowisko przetwarzania w Rządowej Chmurze Obliczeniowej opartej o tzw. chmurę wspólnotową tzn. o własne CPD administracji publicznej oraz na infrastrukturze będącej w jej posiadaniu, ale z wykorzystaniem narzędzi chmurowych a z drugiej na szerszym otwarciu zamówień dla komercyjnej chmury publicznej opartych o standardy cyberbezpieczeństwa. Wydaje nam się jednak, że tak nowatorskie i ciekawe rozwiązania jak ZUCH powinno pełnić znacznie ważniejszą rolę w procesie zamawiania komercyjnych usług chmurowych niż proponowana w zmienionej uchwale. Docelowo powinien działać jako platforma zakupu usług chmurowych i ich certyfikacji w oparciu o podstawy ustawowe. Proponujemy również, aby rząd w dialogu ze środowiskiem biznesowym, przygotował rekomendacje dla zamawiających usprawniające proces zakupów

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

chmury np. w formie rekomendacji Prezesa Urzędu Zamówień Publicznych, czy formy umowy ramowej.
Lewiatan z zaniepokojeniem śledzi zamiary wykluczenia lub dyskryminacji amerykańskich dostawców chmury obliczeniowej w pracach związanych z europejskim systemem certyfikacji usług chmurowych w ramach EUCS.

Oparcie działalności Rządowej Chmury Publicznej na Narodowych Standardach Cyberbezpieczeństwa (NSC) poszczególnych usług chmurowych lub ich europejskich odpowiednikach z zastrzeżeniem dot. w**ykorzystanie normy NSC 800-144.**

Postulujemy też by projekt uchwały zawierał wprost mapowanie norm NSC na normy Europejskie co zapobiegnie spekulacjom i dowolnym ocenom jakie normy NSC odpowiadają jakim normom np. ISO?

NSC 800-144 jest tłumaczeniem amerykańskiej normy NIST 800-144 dotyczącej bezpieczeństwa i prywatności w chmurze publicznej. Jest to norma z 9 grudnia 2011 roku, czyli wprowadzona na niemal siedem lat wcześniej niż Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO). Jest to już standard przestarzały i nie odpowiadający wymaganiom rynku UE, nawet jeśli dostawcy mieliby wykazać się zgodnością ze standardami europejskimi. Dużo lepszym wyborem byłoby wykorzystanie standardu ISO 27018.

W kwestii europejskich standardów będących równoważnymi NSC to w grę wchodzą następujące których w których dostawca zapewnia przetwarzanie zgodnie z następującymi normami:
PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji,
PN-EN ISO/IEC 27002,
PN-EN ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze obliczeniowej,
PN-EN ISO/IEC 27018 dotyczące dobrych praktyk zabezpieczania danych osobowych w chmurze obliczeniowej,
PN-EN ISO 22301 dotyczące zarządzania ciągłością działania.

Tam, gdzie normy to przewidują spełnienie ich wymagań stosowanie powinno być potwierdzone certyfikatami będącymi wynikami audytu przeprowadzonego przez niezależną jednostkę certyfikującą akredytowaną w polskim lub europejskim systemie certyfikacji audytora.

Zakres certyfikacji powinien dotyczyć produktu lub usługi jaka jest wykorzystywana przez użytkownika.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

Widzimy też potrzebę doskonalenia niektórych definicji jak „brokera usług chmurowych, która powinna dot. każdego autoryzowanego dostawcę def. chmury obliczeniowej. Wydaje się że „d**efinicja chmury obliczeniowej (IaaS, PaaS, SaaS)" może nie obejmować dostawców usług kontenerowych czy typu serverless.**

Wydaje się że próba wskazania które z systemów nie mogą być przetwarzane w środowisku chmury publicznej, choć słuszna co do istoty, jest obarczona kilkoma wadami z których najważniejsze to, że wykluczenie dot. informacji niejawnych dot. materii regulowanej ustawą o ochronie informacji niejawnych i nie może być zmieniane uchwała Rady Ministrów. Rozumiemy absolutnie, że informacje niejawne nie mogą trafić do każdej komercyjny chmury obliczeniowej. Można sobie wyobrazić komercyjne rozwiązanie chmurowe działające na terytorium RP które uzyska akredytacje właściwej służby ochrony państwa.

Czy wszelkie dane medyczne objęte rejestrami medycznymi nie powinny trafiać do chmury publicznej? Wydaje się że względy cyberbezpieczenstwa przemawiają za tym by poszukiwać rozwiązań najbardziej bezpiecznych i chroniących prywatność obywateli. Już dziś oferowane są usługi chmurowe w których szyfrowanie zabezpiecza prywatność przetwarzania a usługodawca nie ma dostępu do danych w tym medycznych.

Czy wszelkie rejestru publiczne oparte o ustawę o informatyzacji nie mogą być przetwarzane w chmurze publicznej? Jeżeli np. nie budzi to zastrzeżenie w odniesieniu do rejestru typu Pesel to dlaczego np. lokalna ewidencja ludności nie może być przetwarzana w chmurze publicznej skoro jej centralna postać będzie umieszczona w bezpiecznej chmurze rządowej?

Należy też pamiętać o postulowanym przez Rade i RCB przygotowywaniu planów ewakuacji do chmury i projekcie e-Amabasady. Jeśli wymaganiem pozostałoby wykluczenie publicznej chmury obliczeniowej rejestrów publicznych to wykonując planowanie ewakuacji do chmury obliczeniowej (por. Narodowy Program Ochrony Infrastruktury Krytycznej) taką chmurą może być wyłącznie Rządowa Chmura Obliczeniowa. Oznacza to wielokrotne powiększenie niezbędnych zasobów RChO lub elementów dyskutowanego projektu e-Ambasady, a tym samym dodatkowe koszty. Co więcej, może to nie być tak bezpieczne jak w przypadku ewakuacji do chmury obliczeniowej poza granicami RP w przypadkach zagrożenia klęskami żywiołowymi czy nawet atakami kinetycznymi.

II. Uwagi szczegółowe

1. Par. 2 p. 3) podpunkt b) Definicja chmury obliczeniowej (IaaS, PaaS, SaaS) i wynikająca z tego zmiana w par. 4 ust. 4

Propozycja: wykreślić tę część definicji

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

Propozycja alternatywna: zamienić „trzech modeli dostarczania usług chmurowych (SaaS, PaaS, IaaS),” na „różnych modeli dostarczania usług chmurowych (w szczególności SaaS, PaaS, IaaS)”
Uzasadnienie: określenia modeli SaaS, PaaS, IaaS pochodzą z definicji chmury przygotowanej przez NIST na początku poprzedniej dekady (NIST 800-145). Obecnie chmura obliczeniowa rozwinęła nie tylko te najlepiej znane i najpopularniejsze modele przetwarzania danych, ale także np. technologie kontenerowe lub serverless. Wprowadzanie wyłącznie modeli SaaS, PaaS i IaaS miałoby zatem charakter ograniczający, co nie jest potrzebne.

Z powyższej propozycji wynika także potrzeba zmiany (wykreślenia?) zapisu dotyczącego modeli przetwarzania w par. 4 ust. 4.

2. **Par. 2 p. 13) Wykorzystanie normy NSC 800-144**

Propozycja:
Usunąć z wykazu Narodowy Standard Cyberbezpieczeństwa NSC 800-144

Uzasadnienie:
NSC 800-144 jest tłumaczeniem amerykańskiej normy NIST 800-144 dotyczącej bezpieczeństwa i prywatności w chmurze publicznej. Jest to norma z 9 grudnia 2011 roku, czyli wprowadzona na niemal siedem lat wcześniej niż Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO). Jest to już standard przestarzały i nie odpowiadający wymaganiom rynku UE. Wpisywanie go na listę wymagań jest zbędne, nawet jeśli dostawcy mieliby wykazywać się zgodnością ze standardami europejskimi. Jeśli wprowadzać wymagania związane z wykorzystaniem normy dla podobnego zakresu zagadnień to lepszym wyborem byłoby ISO 27018.

3. **Par. 2 p. 17) Definicja podzielonej odpowiedzialności**

Propozycja: wykreślenie
Uzasadnienie:
Definicja nigdzie nie jest używana. Pojawia się podobne pojęcie w definicji „chmury obliczeniowej”, ale nie odpowiada ono precyzyjnie definicji.
Definicja wprowadza pojęcia nigdzie nie zdefiniowane i nigdzie dalej w treści uchwały niewykorzystywane jak „ustalenia dotyczące odpowiedzialności dostawcy usług „Bezpieczeństwo chmury” i odpowiedzialności odbiorcy usług „Bezpieczeństwo w chmurze” w zakresie: infrastruktury teleinformatycznej, przetwarzania danych oraz

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

usług chmurowych;" – niestety nie jest wskazane co zawierają te ustalenia, trybu ich tworzenia i zmian itd.
Definicji tej nie ma w aktualnie obowiązującej Uchwale WIIP.

4. **Par. 2 p. 18) definicja brokera usług chmurowych oraz zmiana w p. 11) definicja Publicznej Chmury Obliczeniowej**

Propozycja: wykreślenie
Uzasadnienie:
Definicja jest używana tylko raz, wewnątrz definicji „Publicznej Chmury Obliczeniowej" (patrz dalej, propozycja zmiany).
Pojęcie „brokera usług", tak jak zapisane w p. 18 (prawdopodobnie chodzi o przetłumaczone z angielskiego pojęcie „Cloud Service Provider") nie wyczerpuje listy relacji pomiędzy dostawcami chmury obliczeniowej a innymi podmiotami na rynku. Przykładami innych relacji jest sprzedawca (*reseller*), integrator, firma programistyczna (ang. ISV – independent software vendor) i wiele innych.

W świetle powyższego propozycja zmiany p. 11), definicji „Publicznej Chmury Obliczeniowej":
Jest: „… dostępne w modelu chmury publicznej świadczone przez dostawców komercyjnych bezpośrednio lub poprzez brokera usług chmurowych…"

Propozycja: „…dostępne bezpośrednio lub poprzez autoryzowanych partnerów w modelu chmury publicznej od dostawców komercyjnych…"

5. **Par. 3b zmiana zapisu**

Jest:
„§ 3b. Nie dopuszcza się do korzystania z usług przetwarzania w PChO przez:"

Propozycja:
„§ 3b. Dopuszcza się przetwarzanie w PChO z wyjątkiem następujących systemów i rejestrów:"
Wydaje się to być drobną różnicą semantyczną, ale tworzy absolutnie jednoznaczny komunikat dla podmiotów sektora finansów publicznych.
Nie ma potrzeby, oczywiście, zapisywać że przetwarzanie w PChO musi spełniać wymagania opisane w uchwale WIIP oraz inne przepisy prawa.

6. **Par. 3b p.1) Wykluczenie z możliwości przetwarzania w publicznej chmurze obliczeniowej we wskazanych systemach medycznych**

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

Projekt wyklucza:

„Platformę Udostępniania On-Line Usług i Zasobów Cyfrowych Rejestrów Medycznych oraz Elektroniczną Platformę Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych, o których mowa w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2022 r. poz. 1555, 2280 i 2705 oraz z 2023 r. poz. 650 i 1234);"

Propozycja: usunąć to wykluczenie.

Uzasadnienie:

a. Procedowanie i szybkie wejście w życie. ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY w sprawie europejskiej przestrzeni danych dotyczących zdrowia (EHDS),
   Finalne uzgodnienie i ogłoszenie Rozporządzenia jest przewidywane na 2024 rok, a operacyjnie powinno być w mocy w 2025 roku. Wejście w życie Rozporządzenia oznacza konieczność dostosowania do niego wymagań, w tym także liczby potencjalnych użytkowników, bezpieczeństwa dostępu itd. Wykluczenie rozwiązań chmurowych może być w tym przypadku przyczyną gwałtownego wzrostu kosztów i złożoności projektów związanych z danymi medycznymi.

   Jednym z fundamentalnych powodów wprowadzenia EHDS jest transgraniczność wymiany danych dotyczących zdrowia oraz dostępu osób fizycznych do ich elektronicznych danych dotyczących zdrowia i kontrolę nad nimi w kontekście opieki zdrowotnej (pierwotne wykorzystywanie elektronicznych danych dotyczących zdrowia), jak również do innych celów, które przyniosłyby korzyści społeczeństwu, takich jak badania naukowe, innowacje, kształtowanie polityki, bezpieczeństwo pacjentów, medycyna personalizowana, statystyka publiczna lub działania regulacyjne (wtórne wykorzystywanie elektronicznych danych dotyczących zdrowia). Ponadto celem jest poprawa funkcjonowania rynku wewnętrznego poprzez ustanowienie jednolitych ram prawnych, w szczególności w zakresie rozwoju, wprowadzania do obrotu i wykorzystywania systemów elektronicznej dokumentacji medycznej zgodnie z wartościami Unii. Por. motywy (1), (18), (19)

b. Spodziewaną i rzeczywistą liczbę danych związanych z danymi medycznymi, a także ich wzrost w najbliższym czasie.
   To odróżnia wskazane rejestry medyczne od innych rejestrów wymienionych w propozycji Uchwały, których wielkość prawdopodobnie nie ulegnie zmianie w takiej skali i tak krótkim czasie. Dzięki publicznej chmurze obliczeniowej będzie

możliwe opanowanie zarówno kwestii wielkości danych, potencjalnego ruchu osób fizycznych związanego z dostępem (patrz wyżej), jak i bezpieczeństwa dostępu.

c. Plan ewakuacji do chmury
Jeśli pozostałoby wymaganie wykluczenia publicznej chmury obliczeniowej to wykonując planowanie ewakuacji do chmury obliczeniowej (por. Narodowy Program Ochrony Infrastruktury Krytycznej) taką chmurą może być wyłącznie Rządowa Chmura Obliczeniowa. Oznacza to konieczność wielokrotnego powiększenia niezbędnych zasobów RChO lub elementów dyskutowanego projektu e-Ambasady, a tym samym dodatkowe koszty.

Mając jednak na uwadze specyfikę danych we wskazanym systemie jego dyspozytor może stworzyć dodatkowe, specjalne wymagania związane z przetwarzaniem danych w publicznej chmurze obliczeniowej.
Również mając na uwadze istotność danych dotyczących osób najważniejszych z punktu widzenia bezpieczeństwa państwa i bezpieczeństwa narodowego (także: ich najbliższych rodzin) ich zbiór może być wyłączony ze zbioru ogólnego i przeniesiony do wydzielonego rejestru/rejestrów w gestii ministra właściwego do spraw obrony narodowej i ministra właściwego do spraw wewnętrznych, a także nadać im odpowiednią klauzulę. Rozwiązaniu temu powinny towarzyszyć odpowiednie dotyczące retencji takich danych np. przejście do ogólnego rejestru po 5 latach po zakończeniu pełnienia ostatniej funkcji publicznej.

7. Par. 6 ust. 3 – zmiana określenia „deklaracja zgodności dostawcy”

Jest:
„3. Potwierdzenie spełnienia wymagań, o których mowa w § 2 pkt 13 lit. a–c lub pkt 15, lub w ich odpowiednikach określonych w europejskim systemie normalizacyjnym, odbywa się po złożeniu przez dostawcę oferującego usługi chmurowe deklaracji, w postaci papierowej lub elektronicznej, o spełnieniu tych wymagań lub uzyskaniu certyfikacji odpowiadającej tym wymaganiom”
Propozycja:
„3. Dostawca oferujący usług chmurowe winien wykazać się spełnieniem wymagań, o których mowa w § 2 pkt 13 lit. a–c lub pkt 15, lub w ich odpowiednikach określonych w europejskim systemie normalizacyjnym lub poprzez uzyskanie certyfikacji odpowiadającej tym wymaganiom”
Uzasadnienie:
Formuła „deklaracja zgodności” niesie za sobą potrzebę tworzenia sformalizowanego dokumentu podpisanego przez właściwego reprezentanta dostawcy.
Problematyczne nie jest stworzenie, ale utrzymywanie aktualności takiego formalnego dokumentu z trzech względów:

a. w formie zawsze aktualnej – dostawcy nieustająco przechodzą audyty i owocuje to kolejnymi certyfikatami, to oznaczałoby tworzenie nawet kilkunastu deklaracji rocznie,
b. w formie powiązanej z określonymi usługami – dla różnych usług są różne certyfikaty,
c. deklaracja może być związana z podmiotem mającym siedzibę poza Polską co nakłada dodatkowe

Metoda wykazywania się spełnianiem wymagań jest sprawdzona w praktyce i nie rodzi problemów (przykład: wymagania na podmioty nadzorowane, które chcą korzystać z chmury obliczeniowej, Komunikat chmurowy KNF z 23 stycznia 2020).
Nie wskazuje się formy wykazania spełnienia wymagań, jednak takie wykazanie powinno być skuteczne.

KL/397/182/AM/2023

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy