AMERYKAŃSKA IZBA HANDLOWA W POLSCE
Spektrum Tower, ul. Twarda 18, 00-105 Warszawa
Tel: (48) (22) 520-5999, e-mail: office@amcham.pl

Warszawa, dnia 28 lutego 2025 r.

Pan Paweł Olszewski
Sekretarz Stanu w Ministerstwie Cyfryzacji

Szanowny Panie Ministrze,

w imieniu Amerykańskiej Izby Handlowej w Polsce (AmCham) oraz jej firm członkowskich dziękuję za zaproszenie do udziału w konsultacjach aktualizacji Standardów Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO). Doceniamy i jednoznacznie pozytywnie oceniamy fakt, że – mimo iż dokument ten nie podlega standardowemu procesowi konsultacji publicznych – Ministerstwo Cyfryzacji zdecydowało się opublikować projekt proponowanych zmian i umożliwić nadesłanie komentarzy dostawców usług chmurowych oraz zrzeszających ich organizacji. Jesteśmy przekonani, że przyczyni się to do podniesienia jakości SCCO z korzyścią dla ogólnego poziomu cyberbezpieczeństwa w Polsce.

AmCham jest organizacją zrzeszającą przedsiębiorców amerykańskich w naszym kraju, reprezentujących jednocześnie jedną z największych grup inwestorów zagranicznych, którzy stworzyli aktywa w Polsce o wartości 239 mld złotych i kreują 327 tysięcy miejsc pracy. Od ponad 30 lat działamy na rzecz rozwoju wzajemnych relacji gospodarczych, a naszą misją jest poprawa klimatu inwestycyjnego i promocji naszego kraju na rynku amerykańskim. Członkami AmCham są w szczególności wszyscy najwięksi amerykańscy dostawcy usług chmurowych działający w Polsce, dlatego kwestia zapewnienia wysokich standardów cyberbezpieczeństwa chmur obliczeniowych należy do istotnych obszarów zainteresowań Izby.

Poniżej przekazujemy stanowisko AmCham do opublikowanego projektu zmian w SCCO:

A. Uwagi ogólne

1. Cel nadrzędny przesyłanych uwag

Celem wszystkich zamieszczonych poniżej uwag jest osiągnięcie jednoznaczności i pewności prawnej, na jaką powinni liczyć gestorzy systemów teleinformatycznych posługując się Uchwałą WIIP[1] i SCCO podczas szacowania ryzyka i wyboru adekwatnego modelu chmury obliczeniowej. Konieczność zachowania transparentności wymagań wynika wprost z zapisu Uchwały WIIP, która w Załączniku nr 2 w punkcie 2 mówi (podkreślenia nasze):

> *W przypadku gdy w wyniku analizy stwierdzona zostanie dopuszczalność utrzymania danego systemu w Rządowej Chmurze Obliczeniowej lub w określonej publicznej chmurze obliczeniowej,* ***system powinien zostać ulokowany w odpowiedniej chmurze****.* ***Niekorzystanie w powyższym przypadku z usług chmurowych wymaga uzasadnienia****.*
> *Do przeprowadzenia analizy zobowiązany jest podmiot odpowiedzialny za system teleinformatyczny.*

Dotychczasową praktyką gestorów była interpretacja wszelkich nieścisłości zapisów lub wymagań na niekorzyść rozwiązań chmurowych.

[1] UCHWAŁA NR 97 RADY MINISTRÓW z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa"

2. Propozycja minimalnych zmian

Mając na uwadze plany opracowania w najbliższym czasie w resorcie cyfryzacji ustawy regulującej stosowanie chmury obliczeniowej uznajemy aktualnie konsultowany dokument nowych SCCO za standard przejściowy. Dlatego też wypracowane przez nas propozycje zmian są minimalne.

3. Informacje vs dane

Projekt SCCO wymiennie korzysta z pojęć „informacje" (często) i „dane" (nieco rzadziej). Europejskie i polskie prawo usług cyfrowych, z wyjątkiem ustawy o ochronie informacji niejawnych, dotyczy w znaczej części „danych".

W przypadku kategoryzacji poziomu SCCO (rozdział 3.2), zwłaszcza w zakresie *„zgodności sposobu i zakresu tego przetwarzania z obowiązującymi przepisami prawa"* gestorzy systemów teleinformatycznych mogą być zagubieni pomiędzy w.w, pojęciami, co ponownie prowadzi do niepewności prawnej i braku jednoznaczności.

Uważamy, że fundamentem tej niespójniści w stosowaniu pojęć „informacja" i „dane" jest wykorzystanie normy NIST jako podstawy dla SCCO, a to z kolei ma związek z amerykańskim podejściem do ochrony, gdzie ochroną obejmuje się informacje, a nie dane. Oczywiście, tak jak zaznaczaliśmy powyżej, w przypadku ochrony informacji niejawnych określenie „ochrona informacji" jest jak najbardziej prawidłowe i powinno być bezwzględnie utrzymane.

Postulujemy przegląd całego projektu SCCO pod kątem takiego używania w.w. pojęć, które powinny zapewnić gestorom systemów teleinformatycznych czytelność i jednoznaczność.

Przykłady wybrane dla zilustrowania problemu (podkreślenia nasze):

Nazwa poziomu SCCO1: *„**Informacje** inne niż prawnie chronione"*
Opis tego poziomu: *„Poziom SCCO1 obejmuje wszystkie **dane** przeznaczone do publicznego udostępnienia"*

A także dalej:

> *Konsekwencje ujawnienia **informacji** innych niż prawnie chronione:*
> *• ujawnienie **informacji** może mieć ograniczony lub poważny niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne;*
> *• nieautoryzowana modyfikacja lub zniszczenie **informacji** będzie miało ograniczony lub poważny niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne;*
> *• zakłócenie dostępu lub możliwości korzystania z **informacji** lub systemu teleinformatycznego będzie miało ograniczony lub poważny niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.*

Jednak już np. przy opisie SCCO2:

> *Przetwarzanie **danych** przez jednostki administracji publicznej jest dozwolone wyłącznie w centrach danych na terenie RP*

Wreszcie chyba najbardziej jaskrawy przykład, ponieważ na poziomie definicji to dane zawierają informacje, a nie odwrotnie:

> *Poziom SCCO2 obejmuje informacje, które w szczególności:*
> *• zawierają dane osobowe podlegające ochronie ustawowej,*

4. Umowy z dostawcami usług chmurowych.

Projekt SCCO kładzie istotny nacisk na indywidualnie określanie warunków umów na usługi

chmurowe, m.in.:

- „*Jednym z wyzwań przy wyborze ofert usług chmur obliczeniowych jest to, że dostawcy usług chmur obliczeniowych mogą oferować domyślną umowę napisaną z perspektywy dostawcy (umowy adhezyjne). Takie domyślne umowy mogą w niewystarczającym stopniu zaspokajać potrzeby odbiorców usług chmur obliczeniowych i choć nie są niedopuszczalne, należy zwrócić na nie szczególną uwagę*" (str. 16 Projektu SCCO);
- „*W zależności od modelu przetwarzania w chmurze obliczeniowej ta odpowiedzialność kształtuje się w różny sposób, co powinny uwzględniać m.in. umowy o świadczenie usług przetwarzania w chmurze" (*str. 8 Projektu SCCO).

Powyższe wynika wprawdzie m.in. z przepisów PZP, pod który podlegają zamawiający z sektora publicznego, apelujemy jednak o uwzględnienienie w Projekcie SCCO specyfiki działalności dostawców komercyjnych w zakresie oferowanych warunków umownych (w istotnej mierze ustandaryzowanych) w kierunku pogodzenia wymogów PZP ze specyfiką rynkową.

5. Metadane

Obecny projekt SCCO nie przedstawia jasno klasyfikacji i wymagań dotyczących przechowywania logów systemowych. Projekt nie rozróżnia pomiędzy treścią klienta a logami systemowymi, co może prowadzić do błędnej interpretacji wymagań dotyczących lokalizacji przetwarzania.
Wiodący dostawcy usług chmurowych wykorzystują logi w skali globalnej do monitorowania wydajności usług, wykrywania incydentów bezpieczeństwa i doskonalenia usług. Takie globalne przetwarzanie jest niezbędne do utrzymania jakości usług i środków bezpieczeństwa.

Rekomendujemy wprowadzenie w dokumencie rozróżnienia między "treścią klienta" (customer content) a "logami systemowymi" (system logs). Wymagania dotyczące przechowywania danych w UE/EOG powinny odnosić się do treści klienta, przy jednoczesnym uznaniu, że logi systemowe mogą być przetwarzane poza tym obszarem w ramach standardowych operacji usług chmurowych, gdy jest to odpowiednio zdefiniowane w umowach z klientami. Takie doprecyzowanie pozwoli dostosować wymagania SCCO do praktyk branżowych, zachowując odpowiednią ochronę danych klienta.

B. Uwagi szczegółowe

1. Poziomy Wymagań Bezpieczeństwa SCCO – postulaty dotyczące nazewnictwa (Rozdział 3.2):

Nowa nomenklatura użyta w Projekcie SCCO lepiej koresponduje z terminologią stosowaną w obowiązujących przepisach, w tym w szczególności w ustawie o informacjach niejawnych. Niemniej, należy postulować dalsze doprecyzowanie zakresu pojęciowego poszczególnych kategorii informacji/danych, z uwagi na ryzyko niespójności i „nachodzenia na siebie" zakresów pojęciowych poszczególnych kategorii:

Dla SCCO1: ***Informacje inne niż prawnie chronione*** (wcześniej: *niekontrolowane informacje nieklasyfikowane*) – należy bardziej szczegółowo określić (np. poprzez wskazanie większej liczby przykładów), czym są „*informacje inne niż prawnie chronione*", w szczególności czy grupa ta wyklucza możliwość przetwarzania danych osobowych. Innymi słowy, należałoby wyjaśnić czy poziom SCCO1 jest ograniczony do danych nieosobowych lub do innych kategorii „niechronionych" (prawnie) danych. Postulat ten uzasdniamy tym, iż w praktyce coraz częściej także dane nieosobowe są (prawnie) chronione różnymi regulacjami. Ponadto, często trudno jest wyodrębnić w różnych stanach faktycznych dane osobowe od danych nieosobowych, a zatem w praktyce może się okazać, że poziom SCCO1 nie obejmuje żadnych danych i kategoria ta jest pusta.

Dla SCCO2: ***Informacje prawnie chronione*** (wcześniej: *kontrolowane informacje urzędowe*) – postulujemy doprecyzowanie, że z zakresu poziomu SCCO2 wyłączone są informacje/dane objęte poziomami SCCO3 i SCCO4(gdyż informacje niejawne objęte SCCO3 i SCCO4 również stanowią informacje prawnie chronione);

SCCO3: brak uwag

Dla SCCO4: ***Informacje niejawne*** (wcześniej: bez zmian) – zwracamy uwagę, że w tym zakresie należy postulować zmianę nazwy z „*informacje niejawne*" na „*informacje niejawne o klauzuli wyższej niż „zastrzeżone" lub równoważnej klauzuli międzynarodowej*". W ślad za art. 1 ust. 1 ustawy o informacjach niejawnych, pojęciem „informacje niejawne" objęte są wszystkie rodzaje klauzul tajności. Tym samym, w przypadku braku zmiany nazwy, a w konsekwencji i zakresu znaczeniowego kategorii dla poziomu SCCO4, zbiór informacji/danych SCCO3 zawierać się będzie w zbiorze informacji/danych SCCO4 i w praktyce może pojawić się wątpliwość jakie poziomy i kategorie bezpieczeństwa należy stosować dla informacji o klauzuli maksymalnej „zastrzeżone" lub równoważnej klauzuli międzynarodowej (a w związku z tym realna będzie tendencja klientów z sektora publicznego do stosowania zwiększonych wymagań bezpieczeństwa).

2. Rekomendacje dla wymaganych zabezpieczeń bezpieczeń oraz lokalizacji CPD (tabela na str. 9):

Dla SCCO 1:
Postulujemy zmniejszenie poziomu zabezpieczeń bazowych do dotychczasowego, tj. niskiego poziomu poufności, maksymalnie umiarkowanego poziomu integralności oraz niskiego poziomu dostępności (tak jak ma to miejsce na str. 9 SCCO ver. 1.0). Projekt SCCO na str. 10 zakłada bowiem generalne zwiększenie tego poziomu do niskiego/umiarkowanego wobec wszystkich atrybutów bezpieczeństwa. Jest to jednak nieuzasadnione biorąc pod uwagę, że zbiór informacji/danych poziomu SCCO1 w Projekcie SCCO nie zmienił się w stosunku do poziomu aktualnego SCCO1;

Dla SCCO2:

- Lokalizacja CPD określona jako: „(…) teren EOG jeżeli respektowane jest prawo UE" jest myląca. Nie jest zrozumiałe rozróżnienie obszaru UE oraz EOG, w sytuacji gdy RODO obowiązuje w ramach EOG, a nie tylko w ramach UE (zbiór SCCO2 obejmuje m.in. dane osobowe podlegające ochronie prawnej na podstawie RODO, które obowiązuje w ramach EOG). Pojawia się zatem wątpliwość dotycząca celowości takiego rozróżnienia (można się domyślać, że Projekt SCCO nakłada taki obowiązek np. celem przeprowadzania dodatkowej analizy prawa państwa z EOG, jednak nie należącego do UE, np. prawa norweskiego – takie oczekiwanie może być jednak nierealne w praktyce do wykonania; nie jest też jasne jakiego zakresu prawa obcego miałaby taka analiza dotyczyć).

- Natomiast fragment „Dla informacji/systemów o kategoriach bezpieczeństwa na poziomie wysokim dla atrybutów bezpieczeństwa: poufność i integralność należy w pierwszej kolejności wykorzystywać centra danych na terenie RP" identyfikujemy jako zbyt daleko idące ograniczenie dla danych objętych poziomem SCCO2 w stosunku do uchwały WIIP. Większość informacji/danych objętych poziomem SCCO2 może się bowiem okazać, że spełnia kategorie bezpieczeństwa na poziomie wysokim (m.in. z uwagi na ostrożnościowe podejście dokonującego analizy ryzyka gestora systemu) i np. może to dotyczyć danych zdrowotnych zawartych w rejestrach medycznych. Tym samym, tak sformułowana rekomendacja może wykluczyć wszelkie usługi PChO zlokalizowane poza RP, a oferowane z terytorium UE/EOG i prezentujące równie wysokie (jeśli nie wyższe) standardy bezpieczeństwa systemów. W konsekwencji, warunek lokalizacji CPD w

RP – jako lokalizacja „pierwszego wyboru" – należy ocenić jako niespójny z intencją oraz brzmieniem zaktualizowanej uchwały WIIP, w której przewidziano, że wybór skorzystania z PChO (w jurysdykcji krajowej lub EOG) powinien być wynikiem analizy gestora systemu, a nie odgórnie sformułowanej rekomendacji zawartej w SCCO. Pozostawienie tak sformułowanego warunku może de facto nie zmienić obecnej sytuacji i skutkować ograniczeniem CDP do tych oferowanych na terytorium Polski. W związku z tym postulujemy zmianę tego warunku w kierunku, który pozostawi możliwość wyboru indywidualnym klientom (gestorom systemów) pomiędzy CPD zlokalizowanymi w RP oraz w UE/EOG, jeśli te drugie spełniają wymagane standardy bezpieczeństwa dla informacji/systemów o kategoriach bezpieczeństwa na poziomie wysokim. Taka zmiana pozwoli na większą elastyczność oraz konkurencyjność usługodawców i będzie w pełni zgodna z przyjętymi w WIIP założeniami.

Dla SCCO3:

- uwagi dotyczące lokalizacji CPD analogiczne jak te sformułowane powyżej dla SCCO2, w szczególności w zakresie zmiany warunku „pierwszeństwa" CPD w RP na rzecz innych centrów w UE/EOG, jeśli te spełniają wymagane standardy bezpieczeństwa;

- dodatkowo postulujemy usunięcie lub doprecyzowanie następujących określeń: „suwerenność danych" oraz „odpowiedni poziom suwerenności danych", gdyż przepisy prawa nie posługują się takimi sformułowaniami, a co za tym idzie brak jest konkretnych wytycznych co do sposobu rozumienia tych pojęć. W efekcie odbiorcy usług z sektora publicznego mogą napotkać trudności w stosowaniu rekomendacji przetwarzania informacji w tym zakresie.

Dla SCCO4:
Postulujemy dookreślenie na jakich zasadach podmioty komercyjne mogą uczestniczyć w tworzeniu i utrzymywaniu chmur prywatnych służących do przetwarzania informacji niejawnych o określonej klauzuli tajności. Działanie to przyczynie się to poprawy konkurencyjności na rynku usług chmurowych i zapewni podmiotom sektora publicznego większy wybór, elastyczność oraz warunki korzystania z najbardziej nowoczesnych rozwiązań chmurowych, w tym w zakresie rozwiązań zwiększających cyberbezpieczeństwo.

3. Opis zakresu stosowania poziomu SCCO2. (Rozdział 3.2.2)

Proponujemy brzmienie przepisu, które w sposób jednoznaczny dla gestorów określi rodzaje danych jakie mogą być przetwarzane w chmurach obliczeniowych na poziomie SCCO2.

Jest:

Poziom SCCO2 obejmuje informacje, które w szczególności:
• zawierają dane osobowe podlegające ochronie ustawowej,
• zawierają tajemnicę przedsiębiorcy, w tym tajemnice branżowe/instytucjonalne podlegające prawnej ochronie,
• mają charakter wrażliwych, prawnie chronionych informacji i danych referencyjnych krajowych rejestrów - określonych w odrębnych przepisach (w tym dane o kluczowym znaczeniu dla bezpieczeństwa publicznego);
• wymagają jednoznacznego oznaczenia jako informacje o ograniczonym dostępie, w szczególności których nieuprawnione ujawnienie może obniżać skuteczność zabezpieczeń stosowanych w systemach administracji rządowej.

Propozycja (wytłuszczenie wskazuje na propozycję konkretnej zmiany):

*Poziom SCCO2 obejmuje **przetwarzanie danych**, które w szczególności dotyczy:*

- ***danych nieosobowych podlegających ochronie prawnej;***
- *danych osobowych,* ***w tym szczególnych kategorii danych osobowych m.in. takich jak dane medyczne, dane edukacyjne, dane osobowe w procesach kryminalnych;***
- *tajemnic przedsiębiorcy, w tym tajemnic branżowych/instytucjonalnych/**zawodowych** podlegających prawnej ochronie,* ***m.in. takich jak tajemnica skarbowa, tajemnica statystyczna, tajemnica lekarska, tajemnica adwokacka i radcowska, tajemnica komunikacji elektronicznej, tajemnica notarialna;***
- *mają charakter wrażliwych, prawnie chronionych informacji i danych referencyjnych krajowych rejestrów - określonych w odrębnych przepisach (w tym dane o kluczowym znaczeniu dla bezpieczeństwa publicznego);*
- *wymagają jednoznacznego oznaczenia jako informacje o ograniczonym dostępie, w szczególności których nieuprawnione ujawnienie może obniżać skuteczność zabezpieczeń stosowanych w systemach administracji rządowej;*
- ***danych w systemach sztucznej inteligencji, w tym w systemach sztucznej inteligencji wysokiego ryzyka oraz w procesach szkolenia modeli i systemów sztucznej inteligencji.***

Proponujemy także dodanie na końcu powyższego akapitu następującego zapisu:

Zastosowanie określonego modelu chmury – jeśli zastosowanie konkretnego modelu chmury obliczeniowej nie jest wykluczone przez przepisy prawa - może wymagać spełnienia dodatkowych warunków organizacyjnych i technicznych.

Uzasadnienie:

(a) Poziom SCCO2 będzie jednym z najczęściej wykorzystywanych w praktyce, stąd też konieczność największego doprecyzowania możliwości stosowania i wymagań dotyczących tego poziomu. Stąd także propozycje enumeratywnie wymienionych danych, jakie mogą być przetwarzane przy tym poziomie zabezpieczeń.

(b) Proponujemy od razu w pierwszym zdaniu wskazać na „przetwarzanie danych", w miejsce dotychczasowych „obejmuje informacje". Taki zapis ułatwi pracę przy szacowaniu ryzyka przez gestorów przy uwzględnianiu innych przepisów prawa dotyczących przetwarzania danych.

(c) Proponujemy wprowadzenie pojęcia „danych nieosobowych podlegających ochronie prawnej" ze względu na wejście w życie Data Act już we wrześniu 2025 roku.

(d) Przetwarzanie danych osobowych w SCCO odpowiada zapisowi w Załączniku nr 1 do Uchwały WIIP w liniach 5-9, 11-12 oraz 14-17. Szczególne kategorie danych osobowych (art. 9 rodo) mogą być również przetwarzane w chmurze obliczeniowej (linia 10 w/w Tabeli). Do tej ostatniej grupy będą należały także wymienione enumeratywnie w naszej propozycji dane medyczne, dane edukacyjne i dane osobowe w procesach kryminalnych. Przetwarzanie wszystkich danych osobowych musi się oczywiście odbywać zgodnie z właściwymi przepisami prawa, co może nakładać na gestora wprowadzenie adekwatnych zabezpieczeń technicznych i organizacyjnych. Wprowadzenie enumeratywnej listy typów danych ma na celu usunięcie wątpliwości co do możliwości stosowania poziomu SCCO2.

(e) Proponujemy wymienić enumeratywnie rodzaje tajemnic podlegających ochronie prawnej, tak aby usunąć wątpliwości co do możliwości stosowania poziomu SCCO2.

(f) Proponujemy wprowadzić dla poziomu SCCO2 przetwarzanie danych w systemach sztucznej inteligencji, w tym także w systemach wysokiego ryzyka.

(g) Proponujemy uznać SCCO2 jako podstawowy poziom bezpieczeństwa przetwarzania danych w przypadku szkolenia (trenowania) modeli i systemów sztucznej inteligencji.

(h) Poziom SCCO2 pozwala na wykorzystanie chmury publicznej, RChO z zabezpieczeniami RKB lub chmury prywatnej. Wykluczenie jakiegokolwiek z tych modeli, w szczególności wykluczenie z postępowania o zamówienie publiczne, powinno wynikać wyłącznie z przepisów prawa.
Patrz uwaga dot. Wykluczenia chmury publicznej dla poziomu SCCO2.

(i) Natomiast może się okazać, że wykorzystanie konkretnego modelu chmury będzie wymagało spełnienia dodatkowych wymagań organizacyjnych i technicznych. Proponowany zapis pozwala na wskazanie gestorom, że niezależnie od kryteriów wynikających z Uchwały WIIP i SCCO powinni także być przygotowani na analizę pod kątem innych wymagań prawa. Warto zwrócić uwagę, że **wszystkie** wymagania, o których mowa są obowiązujące dla każdego z przyjętych modeli chmurowych czy przetwarzania we własnej infrastrukturze (on-prem).

Przykłady:

a. Ochronę danych osobowych w sektorze sprawiedliwości reguluje tzw. DODO, tj. ustawa z dnia 14 grudnia 2018 roku o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości[2] co może wymagać spełnienia przez dostawcę rozwiązania w chmurze określonych tą ustawą wymagań;

b. Cyberbezpieczeństwo przetwarzania danych w Zakładzie Ubezpieczeń Społecznych reguluje m.in. rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA)[3], co nakłada na podmiot świadczący usługi chmurowe do wypełnienia wymagań techniczno-organizacyjnych dla dostawców do takich podmiotów;

c. Podobna sytuacja może dotyczyć podmiotów w sektorze ochrony zdrowia po wdrożeniu Europejskiej przestrzeni danych dotyczących zdrowia (EHDS)[4];

d. Stosowanie systemów sztucznej inteligencji, w szczególności systemów wysokiego ryzyka, podlega szczegółowym rygorom opisanym m.in. w Rozporządzeniu w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji (AI Act)[5].

4. Wykluczenie chmury publicznej dla poziomu SCCO 2 (Rozdział 3.2.2)

Aktualna propozycja postanowienia wykluczającego wykorzystanie chmury publicznej dla poziomu SCCO2 nie bazuje na wymaganiach jednoznacznie opisanych prawem i wprowadza poważną niepewność prawną gestorów przy analizie ryzyka (SCCO rozdział 3.2). Nasze propozycje zmierzają do rozwiązania tej sytuacji, jednocześnie dając zarówno gestorom jak i właściwym organom możliwość znalezienia adekwatnego rozwiązania technicznego dla systemu teleinformatycznego.

Jest (podkreślenia nasze):

*Jeżeli z analizy ryzyka i systemu zarządzania bezpieczeństwem **jednoznacznie** wynika, że **w celu zachowania m.in. suwerenności danych czy też kontroli nad personelem***

[2] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości
[3] Publications Office
[4] Europejska przestrzeń danych dotyczących zdrowia - Komisja Europejska
[5] L_202401689PL.000101.fmx.xml

technicznym *nie można korzystać z usług chmurowych dostawców komercyjnych, przetwarzanie dozwolone jest wyłącznie w centrach danych na terenie RP w ramach RChO + Rządowego Klastra Bezpieczeństwa lub w ramach Chmury prywatnej.*

Niestety, przy braku jakichkolwiek regulacji dotyczących „suwerenności danych" lub też wskazówek w przepisach prawa w jakich okolicznościach „kontrola nad personelem technicznym" będzie niedostateczna, proponujemy by **wykreślić to postanowienie**.

Zwracamy też uwagę, że przesłanka „kontroli nad personelem technicznym", zakładając, że dotyczy personelu technicznego dostawcy chmury, może być niemożliwa do zrealizowania. Nie jest bowiem standardem rynkowym, aby odbiorca usługi sprawował bezpośrednią kontrolę nad zasobami osobowymi i technicznymi (rzeczowymi) dostawcy usługi. W praktyce, zachowanie takiej przesłanki w toku dokonywania oceny ryzyka i systemu zarządzania bezpieczeństwem może spowodować wykluczenie usług dostawców komercyjnych, co stanie się wbrew założeniom i intencji zaktualizowanej uchwały WIIP.

Propozycja rozwiązania:
Proponujemy rozszerzenie treści akapitu szczegółowo omówionego powyżej o zdanie dotyczące możliwości podniesienia wymagań do poziomu SCCO3. To postanowienie idzie naprzeciw idei uznania, że istnieją sytuacje, w których stosowanie wymagań SCCO2 może nie być wystarczające, natomiast przetwarzane dane nie są danymi zawierającymi informacje niejawne w rozumieniu ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych.

Zastosowanie określonego modelu chmury – jeśli zastosowanie konkretnego modelu chmury obliczeniowej nie jest wykluczone przez przepisy prawa - może wymagać spełnienia dodatkowych warunków organizacyjnych i technicznych.

Jeżeli szacowanie ryzyka związanego z cyberbezpieczeństwem dla przetwarzania danych na poziomie SCCO2 wskazuje na duże lub bardzo duże prawdopodobieństwo wystąpienia incydentu krytycznego w podmiocie kluczowym wówczas gestor systemu teleinformatycznego powinien dokonać jego reklasyfikacji do poziomu SCCO3 i ponownie uzyskać opinię właściwego krajowego zespołu CSIRT.

Uzasadnienie propozycji dodatkowego akapitu:

a. Kwalifikacja zmiany poziomu SCCO. Postanowienie jest wprost związane z cyberbezpieczeństwem, czyli tym czego dotyczą Standardy **Cyberbezpieczeństwa** Chmury Obliczeniowej będące elementem Narodowych Standardów **Cyberbezpieczeństwa**.

b. Oparcie kwalifikacji zmiany poziomu SCCO na źródłach prawa. Wymagania związane z cyberbezpieczeństwem są klarownie **opisane prawem** zarówno w ustawie o krajowym systemie cyberbezpieczeństwa (obecnie obowiązującej, jak i proponowanej przy transpozycji Dyrektywy NIS2) jak i innych aktach prawnych takich jak DORA czy EHDS.

   Warto zwrócić uwagę, że proponowany zapis chroni gestora systemu teleinformatycznego by stosować np. standardy cyberbezpieczeństwa, które nie znajdują się w zapisach polskiego prawa lub dopiero są wstępnie dyskutowane, takie jak Gaia-X.

   Warto także zwrócić uwagę, że ustawa o informatyzacji (art. 3 punkt 19) wprost wprowadziła zasadę braku preferencji i braku dyskryminacji rozwiązań informatycznych, a zatem oparcie się w analizie na źródłach prawa pozwala gestorowi uniknąć zarzutu działania poza granicami prawa:

neutralność technologiczna – zasada równego traktowania przez władze publiczne technologii teleinformatycznych i tworzenia warunków do ich uczciwej konkurencji, w tym zapobiegania możliwości eliminacji technologii konkurencyjnych przy rozbudowie i modyfikacji eksploatowanych systemów teleinformatycznych lub przy tworzeniu konkurencyjnych produktów i rozwiązań;

c. Ograniczenie podmiotowe dla zmiany poziomu SCCO. Decyzja o zwiększeniu wymagań cyberbezpieczeństwa powinna dotyczyć wyłącznie **podmiotów kluczowych**, tak jak definiuje je Dyrektywa NIS2 i transpozycja do polskiego prawa w postaci nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Nie wydaje się by taka sytuacja mogła dotyczyć podmiotów publicznych ważnych, zwłaszcza ze względu potencjalnie znacznie wyższe koszty rozwiązań o wyższych wymaganiach cyberbezpieczeństwa.

   Uwaga: Choć zakres podmiotowy Uchwały WIIP jest ograniczony to jednak SCCO będą wykorzystywane w całym sektorze administracji w Polsce jako wykładnia dla stosowania chmury obliczeniowej, czyli również przez podmioty publiczne-ważne (zgodnie z projektem nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa z lutego 2025). Wprowadzenie zatem ograniczenia podmiotowego będzie miało dla nich ogromne znaczenie.

d. Decyzja o zmianie poziomu SCCO bazująca na precyzyjnej analizie #1. Analiza musi wskazywać, że niższe wymagania cyberbezpieczeństwa mogą prowadzić do powstania **incydentu krytycznego**[6] lub jego odpowiednika opisanego w innych aktach prawnych dotyczących cyberbezpieczeństwa (np. „poważnego incydentu związanego z ICT", zgodnie z definicją z DORA[7]). Możliwość pojawienia się incydentu poważnego (incydentu związanego z ICT) nie jest przesłanką do podwyższenia wymagań.

e. Decyzja o zmianie poziomu SCCO bazująca na precyzyjnej analizie #2. Analiza musi wskazywać na **duże lub bardzo duże prawdopodobieństwo wystąpienia incydentu krytycznego**. Podobny sposób analizy jest od lat stosowany w zarządzaniu kryzysowym, por. matryca ryzyka w zarządzaniu kryzysowym[8].

f. Decyzja o zmianie poziomu SCCO bazująca na precyzyjnej analizie #3. Analiza w sposób jednoznaczny powinna wskazywać, że duże lub bardzo duże prawdopodobieństwo wystąpienia incydentu krytycznego dotyczy wyłącznie wykorzystania systemu teleinformatycznego w publicznej chmurze obliczeniowej. Jeśli incydent jest równie prawdopodobny przy każdym rozwiązaniu nie może to stanowić powodu dla wykluczania jakiegokolwiek z rozwiązań.

g. Podniesienie poziomu SCCO zamiast wykluczenia rozwiązań w chmurze publicznej #1
   Wszystkie powyższe przesłanki uzasadniają nałożenie wymagań poziomu SCCO3, czyli **do poziomu równoważnego ochronie informacji niejawnych o**

[6] Definicja z ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (art. 2 pkt 6)
Incydent krytyczny - incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV
[7] Definicja z art. 3 pkt 10 Rozporządzenia DORA;
Poważny incydent związany z ICT – incydent związany z ICT o dużym negatywnym wpływie na sieci i systemy informatyczne, które wspierają krytyczne lub istotne funkcje podmiotu finansowego
[8] Krajowy Plan Zarządzania Kryzysowego, część A, str. 7, Krajowy Plan Zarządzania Kryzysowego - Rządowe Centrum Bezpieczeństwa - Portal Gov.pl

klauzuli „ZASTRZEŻONE". Choć – na co zwracamy uwagę – przetwarzane dane nie zawierają informacji niejawnych.
Uznajemy, że taki poziom ochrony będzie całkowicie wystarczający dla systemów teleinformatycznych, dla których analiza wskazywałaby, że poziom SCCO2 może być niewystarczający. Jeśli rozwiązanie w chmurze publicznej wypełnia wymagania SCCO3 to nie widać powodu, dla którego miałoby być wyeliminowane. Por. zasada neutralności technologicznej.

h. Podniesienie poziomu SCCO zamiast wykluczenia rozwiązań w chmurze publicznej #2.
Logika propozycji jest oczywista – **jeśli wymagania cyberbezpieczeństwa dla poziomu SCCO2 są niewystarczające to należy zastosować wymagania poziomu wyższego, czyli SCCO3**. Dla obu poziomów możliwe są rozwiązania zarówno w chmurze publicznej, RChO+RKB, jak i w chmurze prywatnej. Unikamy w ten sposób wprowadzania kryteriów nieumocowanych w źródłach prawa i stosowaniu „prawa powielaczowego".
Por, Uchwała WIIP, Załącznik nr 2 punkt 2.

i. Opinia właściwego CSIRT poziomu krajowego. Uchwała WIIP w par. 8 wymaga uzyskania opinii właściwego CSIRT poziomu krajowego. W diagramie RMF na stronie 14 SCCO przedstawiono „klasyfikację systemu IT", wg którego opinia właściwego CSIRT poziomu krajowego dotyczy tylko pierwszego kroku, tj. klasyfikacji – przypisania przez gestora systemu do kategorii SCCO. CSIRT nie opiniuje analizy ryzyka ani wdrożonych środków mitygujących ryzyko, nie opiniuje zabezpieczeń, możliwości funkcjonalnych systemu ani wybranego dostawcy usług chmurowych.

j. Wprowadzenie zasady uzyskania ponownej opinii wynika przede wszystkim z tego, że w sposób oczywisty podniesienie wymagań do SCCO3 będzie niosło ze sobą dodatkowe koszty, a zatem zarówno gestor, jak i właściwy CSIRT poziomu krajowego muszą mieć pewność prawidłowości takiej decyzji.

Por, Uchwała WIIP, Załącznik nr 2 punkt 2.

5. Ograniczenia przetwarzania w chmurze dla poziomu SCCO3 (Rozdział 3.2.3)

Proponujemy przeredagowanie przepisu tak aby stał się czytelny, a także proponujemy zmiany dotyczące ograniczenia przetwarzania w chmurze tak by były oparte na przepisach prawa, jak również mogły być stosowane w praktyce państwo-członka NATO.

Jest:

Przetwarzanie danych przez jednostki administracji publicznej jest dozwolone wyłącznie w centrach danych na terenie RP, jeżeli z analizy ryzyka i systemu zarządzania bezpieczeństwem, w szczególności z powodu braku dostępu do informacji niejawnych o maksymalnej klauzuli „zastrzeżone" lub równoważnej klauzuli międzynarodowej przez personel CPD, jednoznacznie wynika, że w celu zachowania m.in. odpowiedniego poziomu suwerenności danych nie jest możliwe korzystanie z usług chmurowych dostawców komercyjnych. W pozostałych przypadkach dopuszczalne przetwarzanie w centrach przetwarzania danych alokowanych na terenie UE. Dopuszcza się centra przetwarzania na terenie EOG jeżeli respektowane jest prawo UE. Należy uwzględniać wymagania dla ochrony informacji niejawnych właściwych do klauzuli przetwarzanych informacji niejawnych. W pierwszej kolejności należy wykorzystywać centra danych na terenie RP.

Propozycja:

Jeśli w systemie teleinformatycznym przetwarzane będą informacje o klauzuli „zastrzeżone" lub równoważnej klauzuli międzynarodowej to przetwarzanie danych przez jednostki administracji publicznej jest dozwolone w centrach danych na terenie RP po akredytacji systemu zgodnie z ustawą z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych i uzyskaniu zgody właściwego organu. Służba Wywiadu Wojskowego może wyrazić zgodę na przetwarzanie danych w centrach danych alokowanych na terenie krajów członkowskich NATO.
W pozostałych przypadkach rekomenduje się przetwarzanie w centrach danych na terenie RP jednak dopuszczalne przetwarzanie w centrach przetwarzania danych alokowanych na terenie UE. Dopuszcza się również centra przetwarzania na terenie EOG jeżeli respektowane jest prawo UE.
Jeśli przepisy prawa wykluczają możliwość stosowania publicznej chmury obliczeniowej wówczas gestor systemu teleinformatycznego powinien w dokumentacji załączyć opinię właściwego krajowego CSIRT potwierdzającą konieczność wykorzystania Rządowej Chmury Obliczeniowej i Rządowego Klastra Bezpieczeństwa lub chmury prywatnej. W przypadku chmury prywatnej gestora środki organizacyjne i techniczne cyberbezpieczeństwa nie mogą być gorsze niż Rządowej Chmurze Bezpieczeństwa i Rządowym Klastrze Bezpieczeństwa, a gestor powinien dysponować własnym SOC lub usługą SOC-as-a-Service.

Należy także odpowiednio poprawić odpowiednie zapisy w tabeli w pierwszej części Rozdziału 3.2.

Uzasadnienie:

a. Pierwszy akapit naszej propozycji odpowiada zapisom ze znowelizowanej Uchwały WIIP, Załącznik nr 2, ust. 1, linia 2. Proponujemy pozostawić bardziej ogólne określenie o zgodzie właściwego organu, choć w chwili obecnej Uchwała WIIP dopuszcza przetwarzanie informacji o klauzuli „zastrzeżone" wyłącznie dla zadań, które nadzoruje Służba Kontrwywiadu Wojskowego.

b. W przypadku przetwarzania informacji o klauzuli „zastrzeżone" wymagane jest przetwarzanie na terenie RP.

c. Proponujemy zapis, który pozwala SKW na wyrażenie zgody na przetwarzanie informacji o klauzuli „zastrzeżone" także na terenie krajów członków NATO. Opcjonalnie można także dodać kraje UE, ponieważ nie wszystkie są równocześnie członkami NATO np. Austria, Irlandia, Cypr i Malta.

d. Dla poziomu SCCO3 (patrz dyskusja dot. poziomu SCCO2) przetwarzanie danych innych niż zawierających informacje niejawne dopuszczalne jest na terenie krajów UE lub EOG, jednak zachowana jest rekomendacja by przetwarzanie miało miejsce na terenie RP.

e. Jeśli przepisy prawa uniemożliwiają wykorzystanie publicznej chmury obliczeniowej wówczas – po uzyskaniu przez gestora opinii właściwego CSIRT poziomu krajowego potwierdzającej ten fakt – system teleinformatyczny powinien być umieszczony w RChO+RKB lub chmurze prywatnej. Jeśli gestor decyduje się na wykorzystanie chmury prywatnej to warunki ochrony nie mogą być gorsze niż te, które oferuje RChO+RKB, zaś gestor powinien mieć własny SOC lub uruchomioną usługę SOC-as-a-Service.

   Wskazujemy tutaj, że wykluczenie publicznej chmury obliczeniowej może nastąpić wyłącznie na podstawie przepisów prawa.
   Ponieważ rozwiązanie, które będzie wymagało użycia RChO+RKB lub chmury prywatnej z odpowiednimi zabezpieczeniami może być nawet znacząco droższe niż rozwiązanie w chmurze publicznej stąd decyzja gestora musi być potwierdzona przez właściwy CSIRT poziomu krajowego.

A wreszcie, poziom ochrony w chmurze prywatnej gestora musi odpowiadać co najmniej temu jaki jest dostępny w RChO+RKB.

6. Etapy cyklu Risk Management Framework (str. 13-17, w tym rysunek):

Krok 2: Selekcja, wskazano m.in. na wymóg negocjacji umowy definiującej poziom usług i wymagań bezpieczeństwa. Postulujemy w tym zakresie uwzględnienie perspektywy komercyjnych dostawców, którzy oferują produkty wystandaryzowane, z jednolitymi parametrami SLA oraz środkami bezpieczeństwa.

Krok 3: Implementacja, konsekwentnie, postulujemy uwzględnienie ww. specyfiki usług od dostawców komercyjnych. W tym przypadku wdrażanie dodatkowych zabezpieczeń zależy od klienta wdrażającego usługi chmurowe w swej organizacji, z uwzględnieniem powszechnego w ramach usług chmurowych modelu tzw. „współdzielonej odpowiedzialności"; ang. *shared responsibility*, do którego to modelu odnosi się zresztą sam projektodawca w pkt 4.1 Projektu SCCO, str. 17-19).

7. Wymagania bezpieczeństwa w zakresie jurysdykcji (rozdział 5.2)

W zakresie obowiązku przedstawienia listy wszystkich fizycznych lokalizacji centrów przetwarzania danych (na żądanie odbiorcy usługi przed zawarciem umowy; str. 22 Projektu SCCO) – postulujemy doprecyzowanie, że taka lista fizycznych lokalizacji powinna ograniczać się do wskazania regionu (ewentualnie kraju) lokalizacji CPD, a nie obejmować podania dokładnych adresów takich lokalizacji, co samo w sobie naruszałoby względy bezpieczeństwa.

C. Uwagi redakcyjne

1. Doprecyzowanie pojęcia „jednostki administracji publicznej"

Praktycznie w całym dokumencie wykorzystuje się pojęcie „jednostki administracji publicznej", np. przy opisie poziomów SCCO. Proponujemy wprowadzić jedno zdanie precyzujące co w Standardach Cyberbezpieczeństwa Chmury Obliczeniowej oznacza to pojęcie.

Propozycja dodania jednego postanowienia w Rozdziale 1.1.:
Standardy Cyberbezpieczeństwa Chmur Obliczeniowych określają wymagania, jakie muszą spełnić:

- *podmioty administracji rządowej zarządzające Centrami Przetwarzania Danych (CPD), w celu ich przyłączenia do Rządowego Klastra Bezpieczeństwa (RKB) lub włączenia do wspólnych zasobów Rządowej Chmury Obliczeniowej (RChO).*
- *podmioty wskazane w §6 ust. 1 uchwały WIIP planujące wykorzystanie lub korzystające z rządowych i/lub publicznych usług przetwarzania w modelach chmur obliczeniowych.*

zwane dalej jednostkami administracji publicznej, a także

- *dostawcy usług chmur obliczeniowych w ramach Publicznej Chmury Obliczeniowej (PChO).*

Uzasadnienie:
SCCO definiuje kto powinien je stosować (Rozdział 1.1)
Standardy Cyberbezpieczeństwa Chmur Obliczeniowych określają wymagania, jakie muszą spełnić:

- *podmioty administracji rządowej zarządzające Centrami Przetwarzania Danych (CPD), w celu ich przyłączenia do Rządowego Klastra Bezpieczeństwa (RKB) lub włączenia do wspólnych zasobów Rządowej Chmury Obliczeniowej (RChO).*
- *podmioty wskazane w §6 ust. 1 uchwały WIIP planujące wykorzystanie lub korzystające z rządowych i/lub publicznych usług przetwarzania w modelach chmur obliczeniowych.*
- *dostawcy usług chmur obliczeniowych w ramach Publicznej Chmury Obliczeniowej (PChO).*

Uchwała WIIP stanowi w par. 6 ust. 1

§ 6. 1. Z usług przetwarzania w Rządowej Chmurze Obliczeniowej lub publicznych chmurach obliczeniowych mogą korzystać:

1) *podmioty sektora finansów publicznych, o których mowa w art. 9 pkt 1–13 ustawy z dnia 27 sierpnia 2009 r. o finan sach publicznych (Dz. U. z 2019 r. poz. 869, 1622 i 1649);*
2) *inne państwowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, banków i spółek prawa handlowego;*
3) *inne niż określone w ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych, państwowe jednostki organizacyjne nieposiadające osobowości prawnej*

Ponieważ nie wszystkie podmioty wymienione w par. 6 Uchwały WIIP są formalnie jednostkami administracji publicznej, a pojęcie „jednostki administracji publicznej" jest wykorzystywane w całym dokumencie, stąd propozycja zapewnienia klarowności. Mamy świadomość, że nie jest to najlepsze formalne rozwiązanie jednak jest najmniej ingerujące w tekst SCCO.

2. Alokacja centrów danych (Rozdział 3.2)

Słowo „alokować" ma podstawowe znaczenie rachunkowo-księgowe, a nie przestrzenne. Proponujemy zapisać „centra danych na terenie X".

3. Nazwy poziomów SCCO (Rozdział 3.2 i pozostałe)

Proponujemy pozostawić wyłącznie numerację od SCCO1 do SCCO4.
Uzasadnienie:

- Uniknięcie dyskusji „informacje" vs „dane". Jeśli przyjmuje się, że SCCO1 to „Informacje inne niż prawnie chronione" natychmiast pojawia się dyskusja czy wprawdzie informacje nie są chronione prawnie, ale dane już tak itd. itp.
- Uniknięcie nieprecyzyjnego lub zbyt ogólnego opisu poziomu
- Prostota. Praktycznie i tak wszyscy będą posługiwali się wyłącznie numerem poziomu SCCO.

4. Rozdział 3.2.1 Ostatni akapit

Proponujemy usunąć. Jest zbędny.

Dziękując za możliwość wzięcia udziału w konsultacjach i przekazania stanowiska AmCham, deklarujemy dalszą gotowość do udziału w procesie legislacyjnym. W razie jakichkolwiek pytań, pozostajemy do dyspozycji.

AMERYKAŃSKA IZBA HANDLOWA W POLSCE
Spektrum Tower, ul. Twarda 18, 00-105 Warszawa
Tel: (48) (22) 520-5999, e-mail: office@amcham.pl

Z poważaniem

Marta Pawlak, dyrektorka ds. prawnych i polityk publicznych