UWAGI

Polskiej Izby Informatyki i Telekomunikacji [PIIT]

do projektu Komunikatu UKNF dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej o charakterze publicznym lub hybrydowym

Polska Izba Informatyki i Telekomunikacji (PIIT) wita z zadowoleniem projekt Komunikatu UKNF mający na celu ułatwienie wdrożenia chmury obliczeniowej w polskim sektorze finansowym. Stworzenie klarownych ram działania, odpowiednich wymagań i procesów jest niezwykle istotne dla wszystkich interesariuszy działających na rynku, zarówno dla podmiotów nadzorowanych, jak i dla dostawców usług chmury obliczeniowej i dostawców rozwiązań bazujących na chmurze obliczeniowej.

Przedstawiamy poniżej listę uwag do przekazanego projektu przygotowaną dzięki pracy wielu członków naszej Izby. Mamy nadzieję, że nasze uwagi znajdą zrozumienie po stronie organu nadzoru a ostatecznie pozwolą na stworzenie jeszcze doskonalszej wersji komunikatu, jak i doprecyzowanie jego relacji do stanowiska UKNF z dnia 16 września 2019 r. dotyczącego outsourcingu.

1. **Rozdział I Definicje. Punkt 1. Podpunkt 1)**
   Propozycja: Rozszerzyć treść tego punktu o zapis na jego końcu w brzmieniu:
   „i do którego odnosi się jedna z regulacji opisanych w pkt. II. 4 niniejszego komunikatu"
   Uzasadnienie: Z definicji jak w projekcie komunikatu można wywieść (gdyż cytowany przepis mówi o zakresie nadzoru a nie podmiotach nadzorowanych) iż rekomendacja odnosi się także do każdej spółki publicznej – art. 1 ust. 2 pkt. 4; co jest znaczącym i niecelowym rozszerzeniem obowiązków takich spółek. Zarówno rekomendacja D jak i M wprost referowały do obowiązków banków, a wytyczne z 16.12.2014 odnoszą się wyłącznie do podmiotów infrastruktury rynku kapitałowego. Krąg adresatów powinien być zatem zawężony do podmiotów, które są adresatami Komunikatu KNF z 23 października 2017 roku – gdzie na str. 1 poprzez wskazanie, które akty komunikat uszczegółowia doszło do jednoczesnego zawężenia adresatów komunikatu.
   Por. także: Rozdział II, punkt 2, gdzie w jednoznaczny sposób komunikat odnosi się do jednostek sektora finansowego

2. **Rozdział I Definicje. Punkt 1. Podpunkt 3)**
   Propozycja: Odróżnić chmurę obliczeniową od sposobu korzystania z chmury obliczeniowej (jak w obecnej definicji) przyjmując definicję z NIST w brzmieniu:
   „pula konfigurowalnych zasobów obliczeniowych (np. serwerów, pamięci masowych, aplikacji lub usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i minimalnym udziale ich dostawcy."
   Uzasadnienie: Biorąc pod uwagę, iż definiujemy polski rzeczownik „chmura obliczeniowa" to powinniśmy odróżnić same zasoby (chmurę) od korzystania z jej właściwości (przetwarzania w chmurze). Skoro zarówno definicja EBA (EBA/GL/2019/02 str.19) jak i poniższa definicja NIST opisują te zasoby tak samo spróbujmy jasno odróżnić te dwa pojęcia.

3. **Rozdział I Definicje. Punkt 1. Podpunkt 4) – uwaga techniczna**
   Jest: 4) chmura obliczeniowa publiczna – chmura obliczeniowa dostępna do użytku publicznego, będąca w posiadaniu i/lub bezpośrednio zarządzana przez dostawcę usług chmurowych
   Propozycja: 4) chmura obliczeniowa publiczna – chmura obliczeniowa dostępna do użytku publicznego, będąca w posiadaniu i/lub bezpośrednio zarządzana przez dostawcę usług chmury obliczeniowej;
   Uzasadnienie: jednolitość nomenklatury w dokumencie. Również: dotychczasowa forma może także być traktowana jako opis dostawcy usługi chmurowej w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa, a komunikat jednak dopuszcza szerszy krąg dostawców dla sektora finansowego.

4. **Rozdział I Definicje. Punkt 1. Podpunkt 4a) – potrzeba dodatkowej definicji**
   Propozycja: Dodać do komunikatu definicję chmury prywatnej. Proponuje – podobnie jak dla definicji chmury publicznej i chmury hybrydowej – skorzystać z definicji NIST.
   Uzasadnienie: ta definicja może być przydatna dla wszystkich podmiotów kontrolowanych, które będą chciały skorzystać z chmury hybrydowej. Obecność definicji pozwoli na uniknięcie poszukiwania własnych definicji i ujednolici sposób pojmowania pojęcia chmury prywatnej na rynku.

5. **Rozdział I Definicje. Punkt 1. Podpunkt 5)**
   Propozycja: wykreślenie ostatniego zdania w definicji – „Chmura hybrydowa zapewnia zgodność technologiczną i prawną przetwarzania informacji między wszystkimi chmurami obliczeniowymi, które ją tworzą”
   Uzasadnienie: Proponujemy wykreślenie ostatniego zdania tej definicji ze względu na to, że (a) definicja NIST SP-800-145 nic nie mówi o zgodności technologicznej i prawnej, a jedynie wskazuje na używanie tej samej technologii dla wszystkich wykorzystywanych chmur, (b) nie wiadomo jak miałaby być mierzona zgodność technologiczna i prawna – czy to oznacza, że ta sama technologia, np. tego samego producenta miałaby być użyta zarówno w chmurze publicznej (chmurach publicznych), jak i chmurze prywatnej

6. **Rozdział I Definicje. Punkt 1. Propozycja wprowadzenia nowego podpunktu**
   Propozycja: ze względu na klarowność tekstu proponujemy wprowadzenie poniższej definicji, a następnie wykorzystanie jej w dalszej części komunikatu (przede wszystkim zastępując zwrot „niniejszy komunikat”)
   „5a) Komunikat - Komunikat Urzędu Komisji Nadzoru Finansowego z dnia (…) dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej o charakterze publicznym lub hybrydowym;”

7. **Rozdział I Definicje. Punkt 1. Podpunkt 6)**
   Jest: „oznacza umowę w dowolnej formie zawartą między podmiotem nadzorowanym a dostawcą usług chmury obliczeniowej,…”
   Propozycja: „oznacza umowę outsourcingu regulowanego w rozumieniu odpowiednich przepisów prawa zawartą między podmiotem nadzorowanym a dostawcą usług chmury obliczeniowej,…”

Uzasadnienie: Postulowane jest doprecyzowanie, że chodzi wyłącznie o outsourcing regulowany przez właściwe przepisy prawa np. art. 6a ustawy prawo bankowe, art. 3 ust. 1 pkt 27 ustawy o działalności ubezpieczeniowej i reasekuracyjnej, etc.
Proponowany zapis pozwoli zapewnić odpowiedni stopień elastyczności tak sformułowanej definicji, a część zadań jakie podmioty nadzorowane mogą przenieść do chmury obliczeniowej nie będą obligatoryjnie objęte niniejszym komunikatem.

8. **Rozdział I Definicje. Punkt 1. Podpunkt 6)**
Propozycja: wykreślenie w ostatnim zdaniu „która służy do wsparcia realizacji procesu, usługi lub zadania, które podmiot nadzorowany realizowałby samodzielnie, gdyby usługa chmury obliczeniowej była niedostępna"
Uzasadnienie: Proponujemy wykreślić ze względu na oczywistość

9. **Rozdział I Definicje. Punkt 1. Podpunkt 7) – uwaga techniczna**
Postulujemy rozważenie stosowania określenia „istotny" lub „kwalifikowany" jako lepiej oddającego istotę tak pojętego outsourcingu.

10. **Rozdział I Definicje. Punkt 1. Podpunkt 7)**
Uważamy za konieczne doprecyzowanie użytych w tej definicji pojęć.

Uważamy, że dla właściwej oceny przez podmiot nadzorowany czy można zastosować outsourcing szczególny jest niezbędne konkretne odwołanie do zapisów wskazujących, jakie czynności są uznane za istotne i ważne, jakie funkcje operacyjne są uznane jako podstawowe lub istotne, w jaki sposób podmiot nadzorowany miałby ocenić możliwość uszczerbku na reputacji oraz co należałoby określić co stanowi znaczące ryzyko dla klienta.
Mamy obawy, że przy tak ogólnych zasadach kwalifikowania działania jako „outsourcing szczególny" może dojść do sytuacji, kiedy w zasadzie każdy outsourcing należałoby za taki uznać. PIIT zakłada, że określenie „szczególny" (tu: w przypadku outsourcingu) ma być stosowane dla szczególnych i wyjątkowych sytuacji, a zatem dla wszystkich przewidzianych czynności tylko około 5-10% będzie miało charakter „szczególny" zaś zdecydowana większość to będzie podstawowa wersja outsourcingu.
Nie jest także jasne na podstawie obecnego zapisu czy outsourcing szczególny będzie miał miejsce w przypadku spełnienia tylko jednej z wymienionych przesłanek czy np. wszystkich łącznie.

Dużą wartością byłoby gdyby UKNF publikował listy czynności jakie na pewno są outsourcingiem szczególnym pozostawiając w pozostałych przypadkach podmiotom nadzorowanym decyzję o odpowiednim zakwalifikowaniu czynności.

Proponujemy dla określenia „podstawowych lub istotnych funkcji podmiotu nadzorowanego" w definicji outsourcingu szczególnego zastosować definicję przyjętą w wytycznych Europejskiego Urzędu Nadzoru Bankowego (EBA) ws. *outsourcingu* z dnia 25 lutego 2019 r. (EBA/GL/2019/02), co zapewne najlepiej byłoby wprowadzić jako oddzielny punkt w definicjach:

„**podstawowe lub istotne funkcje operacyjne podmiotu nadzorowanego** – funkcje operacyjne, w odniesieniu do których awaria świadczonej usługi i/lub naruszenie zasad bezpieczeństwa mogą mieć potencjalny wpływ na podmiot nadzorowany i jego:

i. ciągłość funkcjonowania działalności gospodarczej, a w szczególności działalności regulowanej, reputację lub rentowność;
ii. zdolność do zarządzania ryzykiem i zgodność z obowiązującymi przepisami ustawowymi i wykonawczymi, w tym ciągłość wypełniania warunków zezwolenia lub innych zobowiązań wynikających z właściwych przepisów szczegółowych;"

Podobnie, proponujemy dookreślenie „czynności istotnych lub ważnych dla działalności podmiotu nadzorowanego jako oddzielny punkt w definicjach:

„**czynności istotne lub ważne dla działalności podmiotu nadzorowanego** – czynności podejmowane przez podmiot nadzorowany, które odnoszą się do informacji o kliencie i – w przypadku nieuprawnionego dostępu lub ujawnienia, lub utraty, lub kradzieży informacji o kliencie – mogą generować znaczące ryzyka dla klientów podmiotu nadzorowanego;"

11. **Rozdział I Definicje. Punkt 1. Podpunkt 7)**
Jeśli zostanie utrzymane, w części lub całości, dotychczasowe brzmienie definicji outsourcingu szczególnego to wówczas proponujemy następującą zmianę:
Jest: „awaria świadczonej usługi i/lub naruszenie zasad bezpieczeństwa mogą mieć potencjalny wpływ na podmiot nadzorowany"
Propozycja: „awaria świadczonej usługi i/lub naruszenie zasad bezpieczeństwa mogą mieć potencjalny istotny i negatywny wpływ na podmiot nadzorowany"
Uzasadnienie: wskazuje klarownie w jakich okolicznościach awarii rzeczywiście należy traktować usługę jako usługę outsourcingu szczególnego.

12. **Rozdział I Definicje. Punkt 1. Podpunkt 9) – uwaga techniczna**
Proponujemy wykreślić tę definicję.
Definicja nie wychodzi poza kolokwialne znaczenie terminu ważność informacji. Prosimy zwrócić uwagę zresztą, że można odwrócić i napisać „istotność informacji – ważność informacji dla prowadzenia działalności…" bez szkody dla zrozumienia czego dotyczy.

13. **Rozdział I Definicje. Punkt 1. Podpunkt 11) – uwaga techniczna**
Jest: przechowywanie kopii zapasowych, przechowywanie informacji w bazie danych
Propozycja: przechowywanych kopii zapasowych, przechowywanych informacji w bazie danych

14. **Rozdział I Definicje. Punkt 1. Podpunkt 13)**
Proponujemy na końcu akapitu rozszerzyć definicję o słowa „… i dalszym poddostawcom"

15. **Rozdział I Definicje. Punkt 1. Podpunkt 15) i 16) oraz**
Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 4.1. podpunkt a)

Propozycja: Proponujemy całkowicie wykreślić obydwa parametry z treści komunikatu, zarówno w Rozdziale I Definicje, jak i dalej w Rozdziale VII, p.4.1.
Uzasadnienie: Obydwa parametry pojawiają się w tekście komunikatu wyłącznie raz, a zatem ich definiowanie w Rozdziale I nie musi mieć miejsca. Natomiast proponujemy nie tylko zrezygnować z ich definiowania, ale także z ich zastosowania w komunikacie.
Wartość RTO dla redundantej architektury publicznej chmury obliczeniowej nie ma znaczenia takiego jak w infrastrukturze własnej. Ma zatem zastosowanie co najwyżej do chmury prywatnej, jeśli taka będzie stosowana. Natomiast w zapisach komunikatu stosuje się go w rozdziale poświęconym umowie z dostawcą usług chmury obliczeniowej, a zatem dla chmury publicznej (Rozdział VII, p. 4.1., strona 13). *De facto* zastąpieniem parametru RTO jest stosowanie certyfikacji SOC połączonych z parametrami w umowie SLA.

W przypadku parametru RPO do wyłącznej decyzji podmiotu nadzorowanego należy określenie ryzyk, które nakazują odpowiednią częstotliwość tworzenia kopii zapasowych, a nawet tego czy kopie zapasowe będą tworzone w chmurze czy też w infrastrukturze własnej podmiotu nadzorowanego; ten parametr nie jest zatem elementem relacji pomiędzy dostawcą usługi chmury obliczeniowej a podmiotem nadzorowanym.

Z powyższych względów proponujemy wykreślić oba pojęcia zarówno z Rozdziału I, jak i z Rozdziału VII (p.4.1., strona 13).

Rozdział II Wprowadzenie, punkt 1 – uwaga techniczna
Jest: „Postęp technologiczny w obszarze technologii chmury obliczeniowej o charakterze publicznym lub hybrydowym"
Propozycja: „Postęp technologiczny w obszarze chmury obliczeniowej"
Uzasadnienie: Nie odchodzimy od definicji z Rozdziału I. Postęp technologiczny w obszarze technologii nie brzmi dobrze…

16. **Rozdział II Wprowadzenie, punkt 5, podpunkt 2)**
Propozycja: wykreślenie tego podpunktu
Uzasadnienie: Całkowite odejście od europejskich wytycznych dotyczących korzystania z rozwiązań chmurowych – tak jak zapisane to zostało w omawianym punkcie - będzie skutkowało obniżeniem poziomu harmonizacji i spowoduje powstanie dodatkowych trudności po stornie instytucji działających w Polsce i w Europie. W szczególności, polskie podmioty nadzorowane będą w gorszej sytuacji, jeżeli chodzi o wdrożenie rozwiązań chmurowych, w stosunku do swoich europejskich odpowiedników.
Jednocześnie polskie podmioty nadzorowane w przypadku działania poza granicami Polski będą zobowiązane do stosowania różnych kryteriów i systemów ocen usług chmury obliczeniowej (np. komunikatu dla terytorium Polski oraz wytycznych EBA/EIOPA dla innych terytoriów krajów członkowskich UE) co może skutkować koniecznością utrzymywania wielu systemów dla tej samej czynności bankowej, a tym samym wyższe koszty i gorszą pozycję konkurencyjną.

17. **Rozdział II Wprowadzenie, punkt 6**

Proponujemy zmienić zapis: „ryzyko koncentracji przetwarzania informacji prawnie chronionych znacznej części sektora finansowego fizycznie w tych samych obiektach”
Propozycja: „w przypadku znaczącego ograniczenia konkurencji ryzyko koncentracji przetwarzania informacji prawnie chronionych znacznej części sektora finansowego fizycznie w tych samych obiektach”
Uzasadnienie: Takie zagrożenie uznajemy za bardzo mało prawdopodobne i występujące jedynie przy korzystaniu przez podmioty nadzorowane z niewielkich dostawców usług chmury obliczeniowej lub w przypadku znaczącego ograniczenia konkurencji pomiędzy dostawcami usług chmury obliczeniowej.

18. **Rozdział II Wprowadzenie, punkt 6 – uwaga techniczna**
Jest: „podmioty nadzorowane będą informowały UKNF o zamiarze wdrożenia outsourcingu szczególnego w chmurze obliczeniowej i/lub w celu przetwarzania informacji prawnie chronionych”
Propozycja: wykreślenie „i/lub”

19. **Rozdział IV Wytyczne stosowania punkt 1 podpunkt 1) i 2) – uwaga techniczna**
Jest:
1) przetwarzane informacje należą do informacji prawnie chronionych zgodnie z niniejszym komunikatem i/lub
2) przetwarzanie informacji ma charakter outsourcingu szczególnego zgodnie z niniejszym komunikatem.
Propozycja:
1) przetwarzane informacje należą do informacji prawnie chronionych w rozumieniu niniejszego Komunikatu i/lub
2) przetwarzanie informacji ma charakter outsourcingu szczególnego w rozumieniu niniejszego Komunikatu.

20. **Rozdział IV Wytyczne stosowania punkt 2**
Propozycja: Proponujemy dopisać na końcu tego punktu następujący zapis:
„… przy czym wprowadzenie stosownych mechanizmów bezpieczeństwa powinno uwzględniać skalę prowadzonej przez nich działalności”
Uzasadnienie: Komunikat będzie dotyczył wszystkich podmiotów nadzorowanych, o bardzo różnej wielkości i skali prowadzenia biznesu. Zapis pozwalający na dostosowanie pracy, jaka będzie wymagana od podmiotu nadzorowanego wydaje się być zasadny.

21. **Rozdział IV Wytyczne stosowania punkt 3**
Propozycja: Proponujemy uzupełnić ten punkt o dodatkowe zdanie:
„Obowiązek ten dotyczy umów zawartych po rozpoczęciu stosowania Komunikatu.”
Uzasadnienie: W rozdziale VIII punkt 1 jest wskazany termin poinformowania UKNF w ciągu 90 dni jeśli przetwarzanie w chmurze już ma miejsce, ale zakres tej informacji jest węższy niż opisywany w Rozdziale IV. Ze względu na dalsze działania podmiotów nadzorowanych wobec procesów przetwarzania i relacji z dostawcami i ich ciągłego charakteru różnice pomiędzy procesami rozpoczętymi przed dniem opublikowania komunikatu oraz po tej dacie szybko ulegną zatarciu. Niniejszy zapis ma służyć zmniejszeniu obciążeń podmiotów nadzorowanych.

W przypadku nie przyjęcia niniejszej propozycji proponujemy poszerzenie okresu dla przygotowania odpowiedniej dokumentacji (patrz uwaga dot. Rozdziału VIII punkt 1)

22. **Rozdział V Wytyczne do klasyfikacji i oceny informacji, punkt 1.**
Uważamy, że opis sposobu klasyfikacji i oceny informacji jest zbyt ogólny. Dla jednolitej oceny, zarówno przez podmiot nadzorowany, jak i później przez regulatora, zapis powinien być bardziej szczegółowy lub powinien odwoływać się do odpowiednich informacji referencyjnych. Por. uwagę dotyczącą definicji „outsourcingu szczególnego".

23. **Rozdział V Wytyczne do klasyfikacji i oceny informacji, punkt 3 podpunkt 2).**
Propozycja: Proponujemy rozdzielenie tego punktu i wydzielenie tematu zmiany CPD do oddzielnego podpunktu. Proponujemy następujący zapis tego nowego podpunktu:
„jeśli zmiana CPD dla istniejącej usługi będzie tego wymagała"
Uzasadnienie: jeśli nie zmieniają się żadne istotne warunki związane z wykorzystywaniem innego CPD, np. jest to ten sam region chmury, ta sama jurysdykcja, lub nawet poprawiają się warunki bezpieczeństwa np. dodatkowe zabezpieczenia ciągłości związane z wykorzystaniem nowych pamięci masowych, zwielokrotnionych kontrolerów itd. itp. to dokonywanie takiej kolejnej klasyfikacji i oceny staje się niepotrzebnym obciążeniem biurokratycznym.

24. **Rozdział V Wytyczne do klasyfikacji i oceny informacji, punkt 4**
Jest: „nie rzadziej niż raz w roku"
Propozycja: „nie rzadziej niż raz na dwa lata"
Uzasadnienie: Ze względu na wymogi konieczności prowadzenia klasyfikacji i oceny na bieżąco oraz prowadzenia dokumentacji co wynika ze wszystkich zapisów Rozdziału V proponujemy zmniejszenie częstotliwości wykonywania przeglądu.

25. **Rozdział VI Wytyczne do szacowania ryzyka, punkt 2 podpunkt 1) podpunkt b)**
Propozycja: wykreślenie tego podpunktu
Uzasadnienie: Ocena tak opisanego ryzyka jest czysto uznaniowa. Intencja zapisu jest jasna, natomiast zapis raczej prowadzi do swobodnych spekulacji niż do rzeczywistej oceny ryzyka i ostatecznego podjęcia decyzji.

26. **Rozdział VI Wytyczne do szacowania ryzyka, punkt 2 podpunkt 1) podpunkt d)**
Propozycja: Proponujemy wykreślenie określenia „pozaumowny".
Uzasadnienie: Jeśli dostęp uprawnionych organów (oczywiście nie mówimy o jakimkolwiek innym dostępie!) jest możliwy to wynika on z zapisów prawa, które obowiązuje nawet kiedy nie zostało zapisane w umowie.

27. **Rozdział VI Wytyczne do szacowania ryzyka, punkt 2 podpunkt 1) podpunkt e)**
Propozycja: Dodanie na końcu tego punktu, po przecinku, następującego zapisu:
„w szczególności ograniczenia lub brak możliwości przenoszenia aplikacji i danych pomiędzy chmurami różnych dostawców (przywiązanie do jednego dostawcy)"

28. **Rozdział VI Wytyczne do szacowania ryzyka, punkt 2 podpunkt 1) podpunkt g)**
Prosimy o precyzyjny opis jakiej sytuacji dotyczy zapis tego podpunktu.
Czy chodzi o bezpieczeństwo narzędzi jakimi dysponuje podmiot nadzorowany, a które mogą pochodzić od dostawcy usługi chmury obliczeniowej, jaki i od stron trzecich? Czy chodzi o bezpieczeństwo API jakie jest używane dla rozwiązań osadzonych w chmurze?

29. **Rozdział VI Wytyczne do szacowania ryzyka, punkt 2 podpunkt 1) podpunkt i) – uwaga techniczna**
Jest: „jego podwykonawców"
Propozycja: „jego poddostawców"
Uzasadnienie: nie ma pojęcia podwykonawców w komunikacie

30. **Rozdział VI Wytyczne do szacowania ryzyka, punkt 2 podpunkt 2) podpunkt a)**
Propozycja: Proponujemy rozdzielić podpunkt na dwa. Pierwszy związany z korzystaniem z usług w sposób niezamierzony, oraz drugi związany obecnością w usłudze teleinformatycznej środowisk nie będących pod kontrolą podmiotu nadzorowanego.

31. **Rozdział VI Wytyczne do szacowania ryzyka, punkt 2 podpunkt 2) podpunkt c)**
Propozycja: Proponujemy zapis: „analiza i weryfikacja domyślnych ustawień parametrów konfiguracyjnych usług pod kątem adekwatności dla potrzeb podmiotu nadzorowanego"
Uzasadnienie: Dostawcy usług chmury obliczeniowej zazwyczaj proponują predefiniowane (*default*) usługi, co jednak oznacza wyższe bezpieczeństwo czy zapewnienie np. *privacy by default*. Zagrożeniem będzie wtedy zmiana takich parametrów dokonana przez osobę nie dysponującą najwyższymi kwalifikacjami, a nie utrzymanie parametrów przygotowanych przez dostawcę.

32. **Rozdział VI Wytyczne do szacowania ryzyka, punkt 2 podpunkt 6) podpunkt a)**
Jest: „a) możliwość tworzenia „łańcucha outsourcingowego" powinna być każdorazowo oceniana przez podmiot nadzorowany z perspektywy przepisów szczególnych prawa dotyczących konkretnie realizowanych czynności przetwarzania informacji w chmurze obliczeniowej"
Propozycja: „a) dopuszczalne jest stosowanie „łańcucha outsourcingowego" o ile nie jest on wprost zakazany przez przepisy prawa lub umowę outsourcingu, jednak możliwość jego tworzenia powinna być każdorazowo oceniana przez podmiot nadzorowany z perspektywy przepisów szczególnych prawa dotyczących konkretnie realizowanych czynności przetwarzania informacji w chmurze obliczeniowej;"
Uzasadnienie: Zasadne jest jednoznaczne wskazanie, że „łańcuch outsourcingowy" jest dopuszczalny.

33. **Rozdział VI Wytyczne do szacowania ryzyka, punkt 2 podpunkt 6) podpunkt b)**
Propozycja:
„należy określić zakres odpowiedzialności dostawcy usług chmury obliczeniowej wobec podmiotu nadzorowanego za szkody wyrządzone umyślnie lub w wyniku rażącego niedbalstwa, z wyłączeniem zdarzeń wynikających z siły wyższej i wynikający z odpowiednich przepisów prawa dla poszczególnych segmentów sektora finansowego oraz wynikający

z rodzaju zastosowanej chmury obliczeniowej; w szczególności kiedy przetwarzanie ma charakter outsourcingu szczególnego"
Uzasadnienie: Propozycja wynika ze względu na różne przepisy dotyczące odpowiedzialności podmiotów nadzorowanych objętych tym komunikatem, ale należących do różnych segmentów (bankowy, ubezpieczeniowy itd.) oraz swobodę kształtowania umów, ale także różne formy chmury obliczeniowej (IaaS, PaaS, SaaS, chmura publiczna, chmura hybrydowa) i związanym z tym podziałem odpowiedzialności pomiędzy dostawcą chmury a jej użytkownikiem (podmiotem nadzorowanym).

Ograniczenie zatem nie powinno mieć szerszego zastosowania niż wynika to z przepisów ustawowych, w związku z czym proponuje się odpowiednie dostosowanie treści komunikatu, z tym doprecyzowanie co do wystąpienia siły wyższej.

Propozycję dodatkowo uzasadniamy faktem, że definicja outsourcingu szczególnego nie jest bardzo precyzyjna (patrz uwaga powyżej).

34. **Rozdział VI Wytyczne do szacowania ryzyka, punkt 2 podpunkt 6) podpunkt c)**
Propozycja: wykreślenie tego punktu
Uzasadnienie: Zgodnie z definicją zamieszczoną w Rozdziale I poddostawcą jest każdy podmiot i/lub osoba, która świadczy usługi. A zatem przy szacowaniu ryzyka trzeba brać pod uwagę obecność wszystkich poddostawców, a nie tylko tych wymienionych w tym podpunkcie.
Tego typu wskazań brakuje także w Wytycznych EUNB w sprawie outsourcingu z 25 lutego 2019 r.

35. **Rozdział VI Wytyczne do szacowania ryzyka, punkt 2 podpunkt 7) podpunkt a)**
Propozycja: „a) prawem właściwym dla umowy jest prawo polskie lub prawo innego państwa członkowskiego Unii Europejskiej"
Uzasadnienie:
    a. Dla podmiotów nadzorowanych, w tym w szczególności polskich firm sektora finansowego, które prowadzą lub planują ekspansję zagraniczną, zapis ograniczający możliwość korzystania tylko z rozwiązań chmurowych bazujących na polskim prawie właściwym będzie istotnym ograniczeniem i może wiązać się z koniecznością poniesienia większych kosztów ze względu na inne rozwiązania teleinformatyczne jakie będą musiały wdrażać w różnych krajach. Poszerzenie możliwości stosowania również prawa innego kraju członkowskiego Unii Europejskiej powinno znacząco ten problem uprościć.
    b. Dla wielu podmiotów nadzorowanych, które są również członkami międzynarodowych grup finansowych, będziemy mieli do czynienia z wykorzystaniem wspólnych usług bazujących na chmurze. W tym przypadku dopuszczenie usług bazujących na prawie jednego z krajów członkowskich Unii Europejskiej będzie zaletą i dopuszczalnym wspólnym mianownikiem.
    c. Dyrektywa NIS i później wdrażająca ją na terenie Rzeczpospolitej ustawa o krajowym systemie cyberbezpieczeństwa przewiduje z definicji korzystanie z usług ponadgranicznych w przypadku wykorzystania dostawców usług cyfrowych (tu: dostawcy usług chmury obliczeniowej), a zatem nawet w szczególnych przypadkach (usługa kluczowa!) ze względu na bezpieczeństwo państwa. Patrz także uwaga do punktu 6.3.

d. Wielu renomowanych dostawców usług chmurowych to podmioty międzynarodowe, które dla ustandaryzowania zasad świadczenia usług online poddają zapisy swoich umów jednemu z praw UE. Często nie jest to prawo polskie. Proponujemy zmianę zapisów i dopuszczenie prawa kraju członkowskiego Unii Europejskiej o ile zapisu umowy i sposób świadczenia usług spełniają wymagania zawarte w komunikacie.

36. **Rozdział VI Wytyczne do szacowania ryzyka, punkt 2 podpunkt 7) podpunkt b) – uwaga techniczna**
Jest: „b) w przypadku poddania umowy prawu państwa trzeciego…"
Propozycja: „b) w przypadku poddania umowy prawu państwa innego niż wskazane w punkcie 7 a) powyżej…"

37. **Rozdział VI Wytyczne do szacowania ryzyka, punkt 5**
Propozycja: W związku z tym, że szacowanie ryzyka jest prowadzone w sposób ciągły (patrz zapisy p.1: „Szacowanie ryzyka jest prowadzone w sposób ciągły") to proponujemy, aby okresowa weryfikacja i aktualizacja była prowadzona raz na dwa lata, a nie raz na rok jak to zapisano w projekcie.

38. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 3.2.**
Jest: „rozumienie konsekwencji"
Proponujemy: „ocenę konsekwencji"

39. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 3.3.**
Jest: „3.3. Kompetencje pracowników i/lub współpracowników podmiotu nadzorowanego odpowiedzialnych za bezpieczeństwo oraz planowanie, konfigurację i zarządzanie oraz monitoring środowiska chmurowego powinny być potwierdzone odpowiednią dokumentacją szkoleniową i/lub imiennymi zaświadczeniami w zakresie odpowiednim do używanych usług chmury obliczeniowej"
Propozycja: „3.3. Kompetencje pracowników i/lub współpracowników podmiotu nadzorowanego odpowiedzialnych za bezpieczeństwo oraz planowanie, konfigurację i zarządzanie oraz monitoring środowiska chmurowego powinny być w miarę możliwości potwierdzone odpowiednią dokumentacją szkoleniową i/lub imiennymi zaświadczeniami w zakresie odpowiednim do używanych usług chmury obliczeniowej"
Uzasadnienie: Proponujemy zapis „w miarę możliwości" uznając aktualny zapis za zbyt rygorystyczny.

40. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 4.1.**
Propozycja: Proponujemy wykreślenie określenia „na piśmie".
Uzasadnienie: Zgodnie z definicją chmury podaną w komunikacie i bazującą na NIST SP 800-145 korzystanie z chmury to dostęp „na żądanie" (w wersji angielskiej definicja brzmi nawet bardziej dosłownie jako „*self-service*"), a to oznacza, że wymóg każdorazowego uzyskiwania „umowy na piśmie" staje się nieprzystający do cyfrowego świata.

Propozycje:
„sformalizowaną umowę”
„ważną umowę”
Porównaj także definicję „outsourcing chmury obliczeniowej” (Rozdział I), gdzie zapisano, że umowa może być zawarta w dowolnej formie.

41. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 4.1.**
Jest: „która – adekwatnie do używanych usług i zakresu przetwarzanych informacji - zawiera co najmniej:”
Propozycja: „która – adekwatnie do używanych usług i zakresu przetwarzanych informacji - zawiera lub wskazuje odpowiednie źródła informacji, co najmniej:”
Uzasadnienie: Taka propozycja zapisu wynika z faktu, że niektóre z przedstawionych w projekcie w punkcie 4.1. informacji mogą być zmienne w czasie co może (ale absolutnie nie musi!) wpływać na świadczenie usługi chmurowej. Dzięki takiemu zapisowi jest możliwe śledzenie zmian oraz adekwatna reakcja
Przykłady: punkt h) – lista poddostawców; punkt j) – źródła informacji o standardach świadczonych usług; r) – zasady wsparcia itd.
Proponowana zmiana nie wpływa na sposób działania podmiotu nadzorowanego, ani na zmniejszenie informacji jakimi dysponuje.

42. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 4.1. podpunkt a)**
Propozycja: wykreślenie „(z uwzględnieniem parametrów RTO i RPO)”
Uzasadnienie: patrz uzasadnienie w uwadze dotyczącej definicji tych parametrów (Rozdział I)

43. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 4.1. podpunkt c)**
Jest: „c) prawo właściwe umowy (w tym zasady rozstrzygania sporów), w szczególności odniesienie do katalogu sytuacji (i/lub podmiotów), w której możliwe jest żądanie informacji lub dostępu do nich bez wyraźnej zgody podmiotu nadzorowanego, zarówno przez organy administracji krajowej/międzynarodowej jak i przez poddostawców dostawcy usług chmury obliczeniowej;”
Propozycja: „c) prawo właściwe umowy (w tym zasady rozstrzygania sporów)”
Uzasadnienie: relacja z dostawcą chmury obliczeniowej bazuje na samoobsłudze (*„self service”*), co oznacza zestaw podstawowych i niezbędnych informacji związanych z prowadzeniem usługi chmury obliczeniowej. Tworzenie katalogu sytuacji, w których potencjalnie byłby możliwy dostęp organów uprawnionych jest praktycznie niemożliwe bez daleko posuniętej analizy prawnej, w tym analizy relacji pomiędzy Polską lub Unią Europejską a danym krajem, a dodatkowo dla różnych procesów (*workloads*) w chmurze obliczeniowej, dla różnych rodzajów wykorzystania chmury obliczeniowej (SaaS, PaaS, IaaS) byłoby niezwykle uciążliwe, o ile w ogóle możliwe. Co więcej mogłoby się zmieniać w czasie.

Por. także uwaga dotycząca Rozdział VI wytyczne do szacowania ryzyka punkt 2) podpunkt 1) podpunkt d) – uznajemy, że przy analizie ryzyka działania mające na celu ocenę sytuacji związaną z prawem właściwym i możliwymi żądaniami uprawnionych organów jest właściwe

44. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 4.1. podpunkt e)**
    Jest: „e) potwierdzenie zgodności zasad przetwarzania danych osobowych z prawem Unii Europejskiej, o ile ma to zastosowanie"
    Propozycja: „e) potwierdzenie zgodności zasad przetwarzania danych osobowych z prawem Unii Europejskiej, o ile ma to zastosowanie, w tym zasad dalszego podpowierzania danych osobowych poddostawcom zgodnie z odpowiednimi przepisami o ochronie danych osobowych"
    Uzasadnienie: W komunikacie należałoby jednoznacznie wskazać, że korzystanie z podwykonawców (podpowierzenie) jest dopuszczalne. Ma to znaczenie choćby w przypadku, kiedy mamy do czynienia z aplikacją SaaS jednego producenta oprogramowania bazującą na platformie (PaaS) innej firmy.

45. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 4.1. podpunkt f)**
    Proponujemy dodanie na końcu tego punktu stwierdzenia: „… o ile ma to zastosowanie"

46. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 4.1. podpunkt m)**
    Propozycja: Proponujemy precyzyjniejszy zapis tego punktu:
    „m) prawo podmiotu nadzorowanego do przeprowadzenia inspekcji w lokalizacjach przetwarzania informacji, w tym prawo do przeprowadzenia audytu 2-giej lub 3-ciej strony na zlecenie podmiotu nadzorowanego (o ile taka potrzeba wynika z szacowania ryzyka). Bez uszczerbku dla ich ostatecznej odpowiedzialności za działania wykonywane przez dostawców usług w chmurze, w celu bardziej efektywnego wykorzystania zasobów audytu i zmniejszenia obciążenia organizacyjnego spoczywającego na dostawcy usług w chmurze podmiot nadzorowany może realizować prawo do przeprowadzania inspekcji poprzez:
        i) korzystanie z certyfikatów oraz raportów stron trzecich lub raportów z audytu wewnętrznego udostępnionych przez dostawcę usług w chmurze;
        ii) korzystanie z audytów zbiorczych (tj. przeprowadzanych wspólnie z innymi klientami tego samego dostawcy usług w chmurze, audytów przeprowadzanych przez klientów zewnętrznych (w szczególności inne podmioty nadzorowane) lub wyznaczoną przez nich stronę trzecią"

    Uzasadnienie: Proponowane jest wskazanie różnych możliwości realizacji prawa do audytu. Z uwagi na specyfikę usług chmurowych (w tym potencjalne obciążenie organizacyjne dostawcy takich usług, ale także ze względów bezpieczeństwa) zasadne jest wskazanie na możliwość realizacji prawa do audytu w inny sposób niż bezpośrednia („na miejscu") inspekcja (kontrola).

47. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 5.3.**

    Propozycja: Proponujemy skreślenie słowa „przetestowany" w obecnym miejscu oraz dodanie na koniec akapitu zapisu:

    „Plan powinien być przetestowany w kluczowych obszarach pozwalających na weryfikację działania planu na reprezentatywnej części infrastruktury, funkcjonalności i danych"

    Uzasadnienie: określenie słowem „przetestowany" jest rozmyte, gdyż nie określa zakresu tego testu – czy jest to tylko część rozwiązania, a może trzeba przetestować całkowite przeniesienie systemu do innego dostawcy lub do infrastruktury własnej. W przypadku dużych systemów teleinformatycznych to ostatnie oczekiwanie byłoby w zasadzie zamknięciem dyskusji o stosowaniu chmury. Proponowany zapis zakłada z jednej strony racjonalność i praktyczność działań dla podmiotów nadzorowanych, a jednocześnie daje regulatorowi pewność wykonania takich testów.

48. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 6.1. – propozycja najdalej idąca**

    Jest: „6.1. W zakresie świadczonych usług dostawca usług chmury obliczeniowej spełnia łącznie wymagania zapewnienia zgodności swojego działania z poniższymi normami lub ich odpowiednikami w polskim lub europejskim układzie normalizacji:"

    Propozycja: „6.1. W zakresie świadczonych usług dostawca usług chmury obliczeniowej spełnia wymagania zapewnienia zgodności swojego działania z odpowiednimi normami lub ich odpowiednikami w polskim, europejskim lub międzynarodowym układzie normalizacji, dla przykładu:"

    Uzasadnienie: Rozumiemy, że zgodność z określonymi standardami jest pomocna w udokumentowaniu, jakie rozwiązania stosuje dostawca usługi chmurowej, jednak w naszej ocenie ich spełnienie nie musi być wymogiem koniecznym, w szczególności łączne wypełnienie wszystkich wymienionych standardów. Przyjęcie zaproponowanego w Komunikacie rozwiązania rodzi następujące konsekwencje:

    a) wskazane standardy mogą się zdezaktualizować w najbliższej przyszłości lub na wdrożenie ich najnowszych wersji jest stosowany tzw. Okres przejściowy (transition period) wynoszący zazwyczaj trzy lata;

    b) przedstawione podejście stanowi bardzo istotną przeszkodę dla oferowania swoich usług podmiotom nadzorowanym przez polskich dostawców z sektora SMB.

    W zamian, podmiot nadzorowany powinien mieć pełną swobodę przy ocenie rozwiązań stosowanych przez dostawcę usług, na podstawie wszelkich dostępnych informacji, w tym spełnianych standardów, posiadanych certyfikatów oraz informacji zebranych w czasie przeprowadzonych audytów.

49. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 6.1.**

    W przypadku nieuwzględnienia uwagi dotyczącej zmian w punkcie 6.1. przedstawionych powyżej proponujemy określenie normy ISO 20000 jako opcjonalnej (zalecanej) lub wyłączenie tej normy z wymagań.

    Uzasadnienie:

1) Europejskie wytyczne odnoszą się do stosowania standardów bezpieczeństwa, natomiast nie odnoszą się do standardów zarządzania, w tym usługami IT, takich jak ISO 20000;
2) ISO 20000 zostało stworzone przede wszystkim dla wewnętrznych działów IT i usprawnienia zarządzania nimi, natomiast nie zostało w swoich wcześniejszych założeniach przystosowane do chmury;
3) ISO 20000-9 dedykowane dla dostawców chmury obliczeniowej zostało finalnie wycofane w 2015 roku przez ISO przed zatwierdzeniem; patrz https://www.iso.org/standard/65671.html
4) ISO 20000-1: 2018, które w lipcu 2018 roku zastąpiło ISO 20000-1: 2011 jest oczekiwane, że zostanie wdrożone w ciągu trzech lat od czasu publikacji (tzw. *Transition period*), co oznacza, że obecnie tylko niektóre usługi mogą wykazać tym certyfikatem (z oczywistych względów wcześniejsze certyfikaty nie będą już odpowiadały obecnym wymaganiom);
5) ISO 20000, w odróżnieniu od pozostałych wymienionych na liście standardów, nie jest wymaganym standardem w powszechnie stosowanych wymaganiach np. Krajowe Ramy Interoperacyjności;
6) nie wszystkie usługi, nawet u największych dostawców, są certyfikowane dla ISO 20000.

50. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 6.2.**
Propozycja: Proponujemy uzupełnić zapis tego punktu przez dodanie na końcu:
… powszechnie uznanego do oceny CPD, lub wypełniania wymagań co najmniej SOC-2."
Uzasadnienie: Sprawdzanie wymagań dotyczących pojedynczych CPD ma sens wyłącznie dla niewielkich dostawców usług chmury obliczeniowej dysponujących pojedynczymi CPD. Dla oceny dużych dostawców powszechnie stosuje się raporty SOC (Service and Organization Controls), a w szczególności SOC-2 powiązany z pięcioma kryteriami zaufania (*Trust Services Criteria*), które dotyczą nie tylko samych CPD, ale usług świadczonych przez dostawcę, w tym także odpowiednich wymagań związanych z CPD, ich bezpieczeństwem, dostępnością, integralnością, poufnością i ochroną danych osobowych.
Zwracamy uwagę, że komunikat wskazuje SOC 2 jako właściwy certyfikat dla części serwisowej (patrz p. 6.4. poniżej).

51. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 6.3. – najdalej idąca propozycja zmiany**
Propozycja: Proponujemy całkowicie zrezygnować z wymagania, aby CPD dostawcy chmury obliczeniowej znajdowały się na terenie EOG.
Uzasadnienie: Koncentracja wszystkich CPD na terenie EOG może skutkować wzrostem ryzyka dla bezpieczeństwa danych związanym z koncentracją geograficzną danych oraz obniża dostępność usług.

52. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 6.3. – uwaga techniczna**
W przypadku braku akceptacji propozycji przedstawionej powyżej.
Jest: „6.3.CPD zlokalizowane jest na terytorium państwa Europejskiego Obszaru Gospodarczego"
Proponujemy zapis „są" zamiast „jest".

Uzasadnienie: wykorzystanie usług chmurowych, którego dostawca ma potencjalnie tylko jeden CPD wydaje się być ryzykowne…

53. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 6.3 podpunkt a)**
W przypadku braku akceptacji przedstawionej powyżej propozycji usuwającej wymaganie korzystania przez podmiot kontrolowany z CPD na terenie EOG.
Proponujemy wykreślić punkt a) z treści Komunikatu.
Uzasadnienie:
1. Charakter dostawców usług cyfrowych (DUC, tu: dostawców usług chmury obliczeniowej) dla operatorów usług kluczowych reguluje ustawa o krajowym systemie cyberbezpieczeństwa (uksc) będąca wdrożeniem dyrektywy 2016/1148 (tzw. Dyrektywy NIS)
2. Dyrektywa NIS w motywie (49) w jednoznaczny sposób wskazuje na transgraniczny charakter usług świadczonych przez DUC i nakazuje zharmonizowane podejście do wymagań nakładanych na te podmioty. Ich praktycznym wyrazem jest rozporządzenie 2018/151.
3. Uksc również nie ogranicza w żaden sposób lokalizacji CPD (rozdział 4), zaś nadzór nad dostawcami usług cyfrowych sprawuje i ma wszelkie narzędzia do odpowiedniego wykorzystania prerogatyw ustawy minister właściwy ds. informatyzacji (dziś: Minister Cyfryzacji). Pozwala to ministrowi właściwemu ds. informatyzacji – w porozumieniu z organem właściwym ds. cyberbezpieczeństwa dla sektora finansowego, czyli UKNF - sprawować bardzo daleko posuniętą kontrolę nad dostawcami usług cyfrowych.
4. Powyższe punkty oznaczają, że zarówno europejski, jak i polski ustawodawca uznali, że zharmonizowane wymagania bezpieczeństwa będą wystarczające dla świadczenia usług kluczowych, w tym w szczególności usług kluczowych świadczonych z wykorzystaniem Dostawców Usług Cyfrowych.

54. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 6.3 podpunkt b)**
Proponujemy - po wykreśleniu podpunktu a) - uzupełnienie na końcu zapisu punktu 6.3. dotyczącego już wyłącznie obiektów i usług infrastruktury krytycznej co najmniej o następujący zapis:
„… na terenie Rzeczpospolitej Polskiej, o ile takie działanie nie jest ograniczone przez przepisy prawa takie jak ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej".

Uzasadnienie: Przywołane Rozporządzenie w artykule 4 zakazuje nakładania wymogów lokalizacji danych nieosobowych, chyba że jest to dozwolone przy zachowaniu odpowiedniej procedury pomiędzy państwem członkowskim a Komisją Europejską.
Wydaje się zresztą, że treść Komunikatu, jeśli zostaną zachowane zapisy dotyczące preferencji lokalizacji na terenie RP, powinien być zgłoszony do Komisji Europejskiej zgodnie z procedurami opisanymi w przywołanym wyżej Rozporządzeniu.

55. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 6.4 podpunkt b)**
Propozycja: „„Brak stałego konta administratora lub użytkownika dostępnego bez ograniczeń dla pracowników dostawcy usługi chmury obliczeniowej lub poddostawców. Zapis ten nie dotyczy kont usług wykonujących automatyczne operacje na danych w imieniu podmiotu nadzorującego."
Uzasadnienie: Zapis w obecnej formie może być rozumiany zbyt restrykcyjnie - dostawca musi posiadać w ramach świadczonych usług chmury obliczeniowej konta serwisowe z dostępem administracyjnym, aby mógł te usługi świadczyć i nimi zarządzać. Podpunkt c dobrze obrazuje intencje regulatora, stąd także propozycja zmiany podpunktu b)

56. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 6.4 podpunkt c)**
Jest: „c) zasadę „minimum koniecznego" dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez oraz na czas ich trwania, przy czym realizacja czynności poprzedzona jest zleceniem podmiotu nadzorowanego"
Propozycja: „c) zasadę „minimum koniecznego" dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez oraz na czas ich trwania lub w celu usunięcia usterki wykrytej przez dostawcę, przy czym realizacja czynności poprzedzona jest zleceniem podmiotu nadzorowanego"
Uzasadnienie: Uzupełnienie o dodatkową możliwą sytuację, kiedy to dostawca może prosić podmiot nadzorowany o możliwość dostępu.

57. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 6.5**
Proponujemy wykreślić.
Najprawdopodobniej nie istnieje jeden certyfikat zgodności, który pokrywałby wszystkie wymienione w Komunikacie wymagania.

58. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 7.2**
Propozycja: Proponujemy uproszczenie zapisu tego punktu do:
„7.2.Podmiot nadzorowany powinien zapewnić, że informacje są szyfrowane kluczami generowanymi i/lub dostarczonymi oraz zarządzanymi przez podmiot nadzorowany lub przez dostawcę usług chmury obliczeniowej."
Uzasadnienie: jest oczywiste, że wybór kluczy musi nastąpić po analizie ryzyka i nie ma potrzeby tego zapisywać.

59. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 7.3**
Jest: „7.3. Podmiot nadzorowany zapewnia, że używane algorytmy szyfrowania nie są powszechnie uważane za skompromitowane"
Propozycja: „Podmiot nadzorowany stosuje algorytmy, które spełniają normę FIPS-140-2 https://csrc.nist.gov/publications/detail/fips/140/2/final, zweryfikowane w programie CMVP

https://csrc.nist.gov/Projects/cryptographic-module-validation-program spełniające rekomendacje CIS https://www.cisecurity.org/cis-benchmarks/ lub STIG"
Uzasadnienie: Ponieważ z dotychczasowego zapisu nie wiadomo, co może oznaczać określenie „powszechnie uważane za skompromitowane" (powszechnie? Od kiedy coś jest uznane powszechnie? Są skompromitowane czy tylko są uważane za skompromitowane?), jak również zakłada, że podmiot nadzorowany może w ogóle chcieć stosować takie algorytmy stąd bardziej precyzyjna propozycja.

60. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 8.4. podpunkt b) – uwaga techniczna**
Jest: „b) podmiot nadzorowany wymusza używanie przez personel dostawcy usług uwierzytelnienia MFA, przy czym rodzaj i zakres uzależniony jest od wyników szacowania ryzyka;"
Propozycja z uzasadnieniem: Jako reprezentanci dostawców żywimy pewne obawy przed metodami wymuszania jakie zostaną zastosowane przez podmioty nadzorowane na naszym personelu stąd proponujemy zmianę w tym zapisie na „podmiot nadzorowany wymaga od dostawcy, aby personel tego ostatniego używał usług uwierzytelnienie MFA" …

61. **Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, punkt 9.1. podpunkt c)**
Ze względu na jednolitość podejścia i późniejszej oceny systemów teleinformatycznych wykorzystujących usługi chmury obliczeniowej KNF powinien przygotować ogólny standard kategoryzacji informacji i systemów. W optymalnej wersji pierwszy taki zbiór zasad powinien być załącznikiem do przedstawionego komunikatu.
Patrz także uwaga dotycząca: Rozdział V Wytyczne do klasyfikacji i oceny informacji, punkt 1.

62. **Rozdział VIII Zasady informowania UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w chmurze obliczeniowej punkt 1.**
Proponujemy: wydłużenie okresu przejściowego do 180 dni
Uzasadnienie: Postulujemy wydłużenie okresu przejściowego dla umów zawartych przed rozpoczęciem stosowania komunikatu z uwagi na konieczność negocjacji ich postanowień na zgodność z niniejszym komunikatem oraz implementację wprowadzonych zmian.
Pozostawiamy do rozważenia również wcześniejszą propozycję (najdalej idącą), aby zasady opisane w komunikacie dotyczyły wyłącznie nowych wdrożeń chmury obliczeniowej.

63. **Rozdział VIII Zasady informowania UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w chmurze obliczeniowej punkt 1. – uwaga techniczna**
Proponujemy zapis: „od rozpoczęcia stosowania" zamiast „od wejścia w życie"
Uzasadnienie: to ostatnie określenie stosuje się do przepisów bezwzględnie obowiązującego prawa – to pierwsze dla wszelkich form soft law.