LEWIATAN

Warszawa, 1 lipca 2021 r.
KL/261/190/AM/2021

Pan
Jacek Jastrzębski
Przewodniczący Komisji Nadzoru Finansowego

Szanowny Panie Przewodniczący,

w nawiązaniu do zaproszenia Komisji Nadzoru Finansowego do przedstawienia uwag do Komunikatu UKNF z dnia 23 stycznia 2020 r. *w zakresie przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej,* które mogą zostać wykorzystane w pracach nad tzw. Q and A (towarzyszącemu Komunikatowi), Konfederacja Lewiatan, w załączeniu, przedstawia stanowisko do dokumentu.

Z poważaniem,

Maciej Witucki
Prezydent Konfederacji Lewiatan

Do wiadomości:
Pan **Zbigniew Wiliński -** Dyrektor Departamentu Innowacji Finansowych FinTech

Załącznik:
Stanowisko Konfederacji Lewiatan - pytania dotyczące Komunikatu UKNF z dnia 23 stycznia 2020 r. w zakresie przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

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

LEWIATAN

Stanowisko Konfederacji Lewiatan - pytania dotyczące Komunikatu UKNF z dnia 23 stycznia 2020 r. w zakresie przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej (dalej: Komunikat)

Konfederacja Lewiatan, poniżej, przedstawia pytania do Komunikatu ze wskazaniem fragmentów Komunikatu, do których się one odnoszą:

I. dostawca usług chmury obliczeniowej – podmiot, który dysponuje infrastrukturą i oprogramowaniem służącym do świadczenia usług chmury obliczeniowej oraz świadczy usługi chmury obliczeniowej;

Pytanie:

Czy dany podmiot powinien wykazać konkretny tytuł prawny, aby spełnić warunek „dysponowania”?

II. Definicja chmury obliczeniowej/tenanta

W kontekście definicji *chmury obliczeniowej* oraz *tenanta* można napotkać na pewne problemy interpretacyjne w usługach, które nie są typowymi przedstawicielami danej grupy (chmura publiczna etc). Można wśród nich wymienić następujące przypadki:

1. Usługa składa się z wielu składników i **część tych składników jest uruchomiona na zasobach usługodawcy (dostawcy usług), pozostała zaś część działa na tzw. VPS (Virtual Private Server) zewnętrznego dostawcy usług chmury obliczeniowej.**

Pytania:

a. **Czy w takim wypadku usługodawca (dostawca usług) staje się zawsze automatycznie dostawcą usług chmury obliczeniowej w rozumieniu Komunikatu?**

b. **Jeśli nie, to jakie powinny być kryteria zakwalifikowania usługodawcy (dostawcy) jako dostawcy usług chmury obliczeniowej w rozumieniu Komunikatu?**

2. Usługa jest posadowiona **w całości w infrastrukturze dostawcy, jednak jest współdzielona pomiędzy wielu klientów**. W takim przypadku odróżnienie usługi chmury obliczeniowej od hostingu może stanowić poważny problem. Spośród przesłanek pozwalających na zakwalifikowanie takiej usługi jako chmury obliczeniowej trudność sprawiają:

a. Poziom separacji klientów. O ile fizyczna separacja nie budzi wątpliwości, jest rzadko spotykana i niepraktyczna, stąd spotyka się separację na poziomie maszyn wirtualnych, kontenerów lub inne. Nie można między nimi jednak postawić znaku równości. Komunikat nie definiuje szczegółowo, kiedy separację można uznać za wystarczającą, aby uznać dwie instancje usługi za osobne tenanty. Wielu mniejszych dostawców usług nie posługuje się nawet pojęciem tenantów, nie identyfikuje również

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

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

siebie jako dostawców usług chmurowych a w procesie analizy danego dostawcy i usługi uzyskanie miarodajnych informacji na temat metod separacji obarczone jest barierą w postaci tajemnicy przedsiębiorstwa i innych. Dodatkowo komunikat zdaje się zamiennie używać pojęcia separacji i izolacji.

Pytanie: Czy pojęcia separacji i izolacji są tożsame w rozumieniu Komunikatu i czy właściwym podejściem jest określenie przez podmiot nadzorowany akceptowalnego poziomu separacji na ogólnie przyjętym, uniwersalnym poziomie abstrakcji tak, aby umożliwić swobodną weryfikację tej informacji (np. separacja na poziomie osobnych instancji maszyn wirtualnych, osobnych obrazów kontenerów, osobnych instancji baz danych czy aplikacji)? Czy UKNF wskazuje minimalny poziom separacji?

b. Współdzielenie zasobów. Podczas analizy architektury usług współdzielenie zasobów przez różnych klientów dotyczy często większej ilości komponentów usługi niż początkowo deklaruje dostawca usługi. Przykładowe komponenty niebrane pod uwagę przy współdzieleniu to urządzenia sieciowe (na wszystkich warstwach modelu OSI, takie jak switche, routery, serwery proxy i loadbalancery, firewalle i analizatory ruchu, wliczając urządzenia klasy SDN i podobne), urządzenia infrastruktury bazowej lub wspomagającej takie jak witalizatory, narzędzia orchestracyjne, infrastruktura DHCP i DNS itp. Uwzględnienie współdzielenia tych zasobów zwiększa prawdopodobieństwo zaklasyfikowania usługi jako chmury obliczeniowej, ale nie ma pewności czy taka jest intencja UKNF.

Pytanie: czy istnieje klasa zasobów, która powinna być brana pod uwagę podczas klasyfikacji usługi jako chmury obliczeniowej pod kątem współdzielenia?

c. Dynamiczność przydzielania zasobów. Dostawcy posiadają zróżnicowane modele obsługi zapotrzebowania na moc obliczeniową swoich platform. Często odbywa się to w hybrydowo, tzn. część zasobów do pewnego limitu jest dostępna automatycznie, natomiast część zasobów w tym powyżej pewnych limitów wymaga ingerencji personelu technicznego. Dodatkowo, przy braku możliwości pełnej weryfikacji tego jak przebiega proces zwiększenia dostępnych zasobów (manualnie, automatycznie czy hybrydowo) jedynym wyjściem wydaje się założenie, że szybko przebiegające zmiany są realizowane automatycznie natomiast długo realizowane zmiany wprowadzane są ręcznie (kwestią otwartą pozostaje kwestia, co oznacza „szybko" i „wolno").

Pytanie: czy istnieje jednoznaczne kryterium spełnienia przesłanki dynamicznego przydzielania zasobów (np. w pełni automatyczne lub przebiegające krócej niż 1h) dla zakwalifikowania usługi jako chmury obliczeniowej oraz czy w razie braku takowego właściwym podejściem jest ustalenie jednego standardowego kryterium na poziomie podejścia do tego zagadnienia przez podmiot nadzorowany?

d. Odniesienie do definicji NIST. Wobec powyższych pytań oraz ogólnej różnorodności usług i występujących przy tej okazji trudności interpretacyjnych pomocna wydaje się dokumentacja NIST definiująca chmurę obliczeniową wzmiankowaną w przypisie do definicji. Nie jest to jednak integralna część komunikatu.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

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

Pytanie: czy uzasadnione i uznawane przez UKNF jest wykorzystanie pełnej treści dokumentu NIST Special Publication 800-145 w celu rozwiania wątpliwości podczas klasyfikacji usług jako chmury obliczeniowej, w szczególności czy właściwym podejściem jest uznanie usługi jako chmury obliczeniowej dopiero po spełnieniu wszystkich 5 kluczowych cech (essential characteristics) z w/w dokumentu łącznie, w jednym z 3 modeli usług (service model) i jednym z 4 modeli wdrożenia (deployment model)?

Z oczywistych względów może istnieć przypadek, który jest kombinacją dwóch powyższych zagadnień. Dlatego liczymy, że udzielone odpowiedzi dadzą się zastosować również w sytuacji hybrydowej.
Źródła:
Pkt. I.1.3) Komunikatu: *chmura obliczeniowa – pula współdzielonych, dostępnych „na żądanie" przez sieci teleinformatyczne, konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci masowych, aplikacji, usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i minimalnym udziale ich dostawcy*[1];
[1] *National Institute of Standards and Technology, Definition of Cloud Computing, Special Publication 800-145.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Pkt. I.1.19 Komunikatu: *tenant – instancja usług chmury obliczeniowej przypisanych do podmiotu nadzorowanego. Najważniejszą właściwością tenantu jest jego domyślna, logiczna separacja (konfiguracji oraz przetwarzanych informacji) od innych tenantów. Każdy pomiot nadzorowany może posiadać wiele tenantów u tego samego dostawcy usług chmury obliczeniowej, jednak wszystkie wymagania związane z separacją tenantów muszą być zachowane.*

III. outsourcing szczególny chmury obliczeniowej
   1. outsourcing szczególny chmury obliczeniowej – oznacza outsourcing chmury obliczeniowej, w ramach którego podmiot nadzorowany powierza dostawcy usług chmury obliczeniowej wykonanie za pomocą usługi chmury obliczeniowej czynności lub funkcji podmiotu nadzorowanego, których brak lub przerwa w realizacji spowodowana awarią lub naruszeniem zasad bezpieczeństwa usługi chmury obliczeniowej, w ocenie podmiotu nadzorowanego:

Pytanie:

W jakich sytuacjach samo korzystanie z mocy obliczeniowej bez powierzenia wykonania żadnych czynności lub funkcji podmiotu nadzorowanego może stanowić outsourcing szczególny chmury obliczeniowej?

   2. Dodatkowo KL proponuję przyjęcie następującej zmiany definicji outsourcingu szczególnego chmury obliczeniowej (elementy dodane zostały pogrubione).

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

outsourcing szczególny chmury obliczeniowej -oznacza outsourcing chmury obliczeniowej, w ramach którego podmiot nadzorowany powierza dostawcy usług chmury obliczeniowej wykonanie za pomocą usługi chmury obliczeniowej czynności lub funkcji podmiotu nadzorowanego, których brak lub przerwa w realizacji spowodowana awarią lub naruszeniem zasad bezpieczeństwa usługi chmury obliczeniowej, w ocenie podmiotu nadzorowanego:

a) wpływałaby w sposób istotny na ciągłość wypełniania przez podmiot nadzorowany warunków stanowiących podstawę uprawnienia prowadzenia działalności nadzorowanej lub jej wykonywania lub
b) zagrażałaby w sposób istotny wynikom finansowym podmiotu nadzorowanego, niezawodności lub ciągłości wykonywania działalności nadzorowanej

3. Definicja outsourcingu szczególnego w Komunikacie a przepisy UFI w zakresie outsourcingu

1. Zgodnie z pkt. I. 1.11) Komunikatu:

*outsourcing szczególny chmury obliczeniowej – oznacza outsourcing chmury obliczeniowej, w ramach którego podmiot nadzorowany powierza dostawcy usług chmury obliczeniowej wykonanie za pomocą usługi chmury obliczeniowej czynności lub funkcji podmiotu nadzorowanego, **których brak lub przerwa w realizacji spowodowana awarią lub naruszeniem zasad bezpieczeństwa usługi chmury obliczeniowej**, w ocenie podmiotu nadzorowanego:*

a. *wpływałaby **w sposób istotny na ciągłość wypełniania przez podmiot nadzorowany warunków stanowiących podstawę uprawnienia prowadzenia działalności nadzorowanej lub jej wykonywania** lub*

b. *zagrażałaby **w sposób istotny wynikom finansowym podmiotu nadzorowanego, niezawodności lub ciągłości wykonywania działalności nadzorowanej.***

2. Zgodnie z art. 45a ust. 8 ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi (UFI):

*Za umowy, których przedmiotem są czynności **niemające istotnego znaczenia dla prawidłowego wykonywania przez towarzystwo obowiązków określonych przepisami prawa, sytuacji finansowej towarzystwa, ciągłości lub stabilności prowadzenia przez towarzystwo działalności**, o której mowa w art. 45, uznaje się w szczególności umowy, których przedmiotem jest:*

1) świadczenie na rzecz towarzystwa doradztwa lub innych usług niezwiązanych bezpośrednio z prowadzoną przez towarzystwo działalnością, o której mowa w art. 45, w tym usług:
a) doradztwa prawnego,
b) szkolenia pracowników,
c) prowadzenia ksiąg rachunkowych towarzystwa,
d) ochrony osób lub mienia;
2) świadczenie na rzecz towarzystwa usług wystandaryzowanych, w tym usług polegających na dostarczaniu informacji rynkowych lub informacji o notowaniach instrumentów finansowych.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

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

Spełnienie powyższych przesłanek powoduje, że mamy do czynienia z tzw. outsourcingiem niekwalifikowanym w kontekście UFI (nazewnictwo własne autora dla ułatwienia interpretacji przepisów), w ramach którego podmiot nadzorowany jest zwolniony z obowiązku stosowania niektórych wymogów, których UFI wymaga (*a contrario)* dla tzw. outsourcingu kwalifikowanego, który wymaga m.in. zawiadomienia KNF przed zawarciem umowy z outsourcerem.

3. Zestawione powyżej definicje, pomijając w tym miejscu specyfikę chmury obliczeniowej, zawierają w swojej istocie **wspólne elementy ocenne**, odnoszące się do istotnego wpływu (znaczenia) outsourcingu na:
   a. wypełnianie obowiązków określonych przepisami prawa, w tym w szczególności przepisami regulującymi podstawy wykonywania działalności nadzorowanej (UFI),
   b. sytuację finansową,
   c. ciągłość wykonywania działalności nadzorowanej.

4. Zważywszy na okoliczności wskazane powyżej:

Pytania:

a. **Czy UKNF dopuszcza sytuację, w której podmiot nadzorowany kwalifikuje usługę chmury obliczeniowej jako outsourcing szczególny chmury obliczeniowej na gruncie Komunikatu (przy założeniu prawidłowej wykładni ww. definicji i jej faktycznej materializacji w danym przypadku), przy jednoczesnym braku zakwalifikowania ww. usługi jako outsourcing tzw. kwalifikowany na gruncie UFI?**

b. **Czy w kontekście odpowiedzi na pytanie zawarte powyżej (lit. a) ma znaczenie fakt, czy Podmiot nadzorowany przetwarza w chmurze obliczeniowej informacje prawnie chronione (tajemnica zawodowa funduszy) czy też nie przetwarza takich informacji (jednak przy założeniu, że zachodzi outsourcing szczególny w rozumieniu Komunikatu).**

4. łańcuch outsourcingowy – relacja polegająca na:

a) powierzeniu przez dostawcę usług chmury obliczeniowej części czynności (służących dostarczaniu usługi chmury obliczeniowej dla podmiotu nadzorowanego) swojemu poddostawcy i dalszym (kolejnym) poddostawcom lub

b) relacja polegająca na dostarczaniu przez dostawcę usług chmury obliczeniowej usługi chmury obliczeniowej innemu dostawcy, który wykorzystuje usługę chmury obliczeniowej do świadczenia własnej usługi dla podmiotu nadzorowanego

Pytanie:

Czy w przypadku gdy usługa chmury obliczeniowej jest zbudowana i utrzymana przez jeden podmiot z grupy kapitałowej, a sprzedawana przez drugi podmiot z grupy kapitałowej, zachodzi łańcuch outsourcingowy czy też tę sytuacje należy traktować jako zwykły outsourcing chmury obliczeniowej? Czy w takiej sytuacji, w świetle regulacji KNF, należy uwzględniać jeden podmiot czy oba?

IV. Wprowadzenie. Pkt 3 na str. 5: Niniejszy komunikat nie wyłącza przepisów bezwzględnie obowiązujących w tym zakresie, natomiast celem jest zaprezentowanie, jak Nadzór rozumie te przepisy.

- Jaki charakter prawny ma Komunikat? Jakie środki prawne przysługują w razie odmiennego zdania na temat interpretacji postanowień komunikatu?

V. Wprowadzenie pkt 6, ppkt. 3) na str. 6: „Niniejszy komunikat jest podejściem krajowym do outsourcingu przetwarzania informacji w chmurze obliczeniowej dla sektora finansowego (model referencyjny). Tym samym: (…)

3) wytyczne, zalecenia lub inne dokumenty prezentujące stanowisko Europejskiego Urzędu Nadzoru Bankowego, Europejskiego Urzędu Nadzoru nad Ubezpieczeniami i Pracowniczymi Programami Emerytalnymi bądź Europejskiego Urzędu Nadzoru nad Rynkami i Papierami Wartościowymi, które odnoszą się do przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej, nie mają zastosowania do podmiotów nadzorowanych w tym zakresie.

- Czy to oznacza, że wytyczne, zalecenia lub inne dokumenty Europejskiego Urzędu Nadzoru Bankowego, Europejskiego Urzędu Nadzoru nad Ubezpieczeniami i Pracowniczymi Programami Emerytalnymi bądź Europejskiego Urzędu Nadzoru nad Rynkami i Papierami Wartościowymi, które odnoszą się do przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej, nie mają zastosowania do podmiotów nadzorowanych w tym zakresie, czy też są sytuacje, gdy podmioty nadzorowane muszą stosować równocześnie postanowienia komunikatu oraz np. wytyczne Europejskiego Urzędu Nadzoru Bankowego? Jakie to sytuacje?

VI. Wytyczne szacowania ryzyka. Str. 11: pkt. 6) stanowisko nadzoru w sprawie tworzenia łańcucha outsourcingowego, zgodnie z którym:

a) tworzenie łańcucha outsourcingowego powinno być każdorazowo oceniane przez podmiot nadzorowany z perspektywy przepisów szczególnych prawa dotyczących konkretnie realizowanych czynności przetwarzania informacji w chmurze obliczeniowej, a w szczególności:

I. tworzenie łańcucha outsourcingowego w zakresie działalności nadzorowanej jest dopuszczalne wyłącznie w granicach przewidzianych przepisami prawa;
II. tworzenie łańcucha outsourcingowego w zakresie innym niż w zakresie działalności nadzorowanej jest dopuszczalne, o ile nie jest wprost zakazane przez przepisy prawa lub postanowienia umowne;

Pytanie:

Czy usługa chmury obliczeniowej stanowi czynność pomocniczą służącą wykonaniu świadczenia głównego (art. 6a ust. 7 pkt. 1 ustawy prawo bankowe), gdy jej treścią jest samo udostępnienie

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

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

mocy obliczeniowej, a ewentualne funkcje lub zadania outsourcowane realizuje strona umowy z bankiem, dla której dostawca chmury jest podwykonawcą?

VII. b) zakres odpowiedzialności dostawcy usług chmury obliczeniowej oraz jego poddostawców wobec podmiotu nadzorowanego może ulegać ograniczeniu albo wyłączeniu wyłącznie w granicach szczególnych przepisów prawa regulujących działalność podmiotu nadzorowanego, przy czym Nadzór krytycznie ocenia takie wyłączenia albo ograniczenia, jeżeli:

i. w ramach usługi chmury obliczeniowej przetwarzane są informacje prawnie chronione szyfrowane za pomocą kluczy szyfrujących dostarczonych lub zarządzanych przez dostawcę usług chmury obliczeniowej lub jego poddostawcę lub

ii. przetwarzanie ma charakter outsourcingu szczególnego chmury obliczeniowej;

Pytania:

Jak to postanowienie ma działać w kontekście łańcucha outsourcingowego? Czy dostawca chmurowy miałby być stroną umowy outsourcingu szczegółowego, czy też może być podwykonawcą?

Co w praktyce ma oznaczać, że „Nadzór krytycznie ocenia takie wyłączenia albo ograniczenia”?

VIII. Bank zawiera umowę z dostawca X, na podstawie której zamierza korzystać z oprogramowania dostarczonego w modelu SaaS, gdzie: aplikację biznesową zapewnia podmiot X (bank zawrze z nim bezpośrednio umowę outsourcingową), platformę niezbędną do działania oprogramowanie podmiotu X (PaaS/IaaS) zapewnia dostawca Y (np. AWS, Microsoft, Google). Mamy do czynienia z przetwarzaniem informacji chronionych. Przedsiębiorcą, z którym bank zawiera umowę, o której mowa w art. 6a ust. 1 pkt 2 prawa bankowego (insourcerem), jest podmiot X:

a) który podmiot jest dla banku dostawca chmurowym w rozumieniu Komunikatu chmurowego (podmiot X, z którym bank zawiera umowę outsourcingową, czy podmiot Y, z którym bank nie ma bezpośredniej relacji ani umowy);
b) której umowy dotyczą wymagania Komunikatu (pkt VII. 4 Umowa z dostawca usług chmury obliczeniowej - umowy bank – X, na której treść bank ma wpływ i z której wynikają prawa i obowiązki dla banku, czy umowy pomiędzy X –Y, której bank nie jest stroną i na podstawie której bank nie ma żadnych praw/roszczeń do dostawcy X ani Y, nie ma wpływu na treść umowy/ jej zmiany w przyszłości)?
c) czy bank powinien żądać ujawnienia treści umowy pomiędzy X i Y i oceniać ją w zakresie zgodności z Komunikatem (pkt VII. 4) mimo że w rzeczywistości bank nie jest stroną tej umowy, nie ma żadnych praw przyznanych na podstawie tej umowy, nie ma wpływu na dalsze zmiany w treści tej umowy?
d) co w sytuacji, gdy X lub Y nie wyrazi zgody na ujawnienie treści zwartej umowy, ale X oświadcza, iż wiążąca go z Y umowa zawiera elementy wskazane w Komunikacie (pkt VII. 4)

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

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

e) jeśli umowa pomiędzy X i Y (bank nie jest stroną tej umowy) jest zawarta na prawie państwa trzeciego, to:
   - czy wymagana jest opinia prawna, o której mowa w pkt VI.2 pkt 8 Komunikatu)?
   - która umowa miałaby być przedmiotem powyższej opinii prawnej?
   - co powinno być poddane szczególnej ocenie w treści powyższej opinii?

f) której umowy i którego dostawcy powinny dotyczyć informacje w notyfikacji do KNF?

IX. Jak należy rozumieć „identyfikowalny dostęp do informacji przetwarzanych przez podmiot nadzorowany"? Czy jeśli poddostawca nie może zapoznać się z treścią informacje, ale może posiadać wiedzę, ze są to informacje należące do konkretnego podmiotu, to jest to identyfikowalny dostęp? Czy można uzyskać przykłady, kiedy dostęp jest identyfikowalny, a kiedy nie?

X. W przypadku nabycia usług związanych z przetwarzaniem w chmurze publicznej informacji prawnie chronionych od Operatora Chmury Krajowej:

a) jaka rolę pełni Operator Chmury Krajowej?

b) czy Operator Chmury Krajowej, z którym bank zawiera umowę, jest dostawcą chmurowym w rozumieniu Komunikatu?

c) nie jest dostawca chmurowych, ale jest dostawcą usług dla banku, który korzysta z podwykonawców (Microsoft, Google) – czy w takim przypadku nie ma ryzyka, że dostawca (Operator Chmury Krajowej, podmiot z którym bank zawarł umowę outsourcingową, zlecił swoim poddostawcom istotę usługi (zakres usług poza zakresem dozwolonym do podzlecenia na podstawie art. 6a ust. 7 prawa bankowego)?

XI. Dostawcy usług chmurowych bardzo często nie zawierają umów bezpośrednio z użytkownikami tych usług, tylko użytkownicy (np. bank, dostawcy usług informatycznych dla banku) zawierają umowę z tzw. resellerem/ składają zamówienie na usługi u reselera. Reseller jest podmiotem, któremu bank albo inny podmiot zleca nabycie/opłacenie określonych usług za określoną kwotę. Zapłata wynagrodzenia z tytułu korzystania z usług chmurowych następuje za pośrednictwem resellera, czasami reseller stanowi pierwszą linię wsparcia w przypadku problemów z usługą, ale reseler nie świadczy usługi przetwarzania danych w chmurze. Jaka jest rola resellera w procesie zawierania umowy outsourcingowej:

a) czy jest on dostawca usługi chmurowej i konsumuje pierwsze ogniowo w tzw. łańcuchu outsourcingowym?

b) czy jest podmiotem nieistotnym dla usługi głównej (nie ma żadnego wpływu na usługę świadczoną przez dostawce chmurowego) i można go pominąć w tzw. łańcuchu outsourcingowym?

c) czy w zakresie zgodności z pkt VII. 4 Komunikatu powinna być badana umowa pomiędzy bankiem a reselerem?

XII. Dostawca usług chmurowych podmiot z siedzibą z USA ma zawartą umowę ramowa (tzw. Master Service Agreement) ze spółką z grupy kapitałowej banku. MSA określa ogólne zasady współpracy, stawki itp. Następnie polski bank i podmiot z grupy dostawcy chmurowego posiadający siedzibę na terenie UE i przetwarzający dane na terenie UE, zawierają tzw. umowę wykonawczą z wykorzystaniem i zastosowaniem postanowień MSA. Czy w takim przypadku:

a) wymagana jest zgoda KNF na zawarcie umowy wykonawcze?;

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

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

b) czy wymagana jest opinia prawna, o której mowa w pkt VI.2 pkt 8 Komunikatu? Co powinno być poddane szczególnej ocenie w treści powyższej opinii?

XIII. czy podmiot realizujący usługi na rzecz dostawcy chmurowego, który nie ma możliwości zapoznania się z informacją prawnie chronioną, ale jest niezbędny do zapewnienia prawidłowego wykonania usługi, nie jest poddostawcą w rozumieniu Komunikatu chmurowego i ustawy prawo bankowe i tym samym może nie być uwzględniony w tzw. łańcuchu outsourcingowym?

XIV. czy w przypadku gdy podmiot realizujący usługi na rzecz dostawcy chmurowego ma siedzibę poza EOG, nie ma możliwości zapoznania się z informacją prawnie chronioną, ale wykonuje część świadczenia głównego/usuwa błędy w usłudze głównej lub w inny sposób przyczynia się do zapewnia prawidłowego działanie usługi, wymagana jest zgoda KNF na zawarcie umowy?

XV. w celu realizacji usługi chmurowej, na podstawie umowy zawartej z podmiotem z siedzibą w EOG, dane z data center w UE muszą być przesłane do data center w USA, ale przesył danych odbywa się na zasadach transmisji danych analogicznych jak transmisja danych telekomunikacyjnych (nie ma żadnych działań na danych, przesył na zasadzie routingu). Data center i infrastruktura w USA jest zarządzane przez amerykański podmiot. Czy na zawarcie umowy z takim modelem przepływu danych jest wymagana zgoda KNF?

XVI. Bank zawarł umowę na korzystanie z usług chmurowych obejmujących przetwarzanie informacji prawnie chronionych, dokonał szacowania ryzyka i notyfikacji zgodnie z Komunikatem na okoliczność pierwszych usług i informacji, które były uruchamiane w rozwiązaniu chmurowym na moment zawarcia umowy i notyfikacji. Po pewnym czasie bank, korzystając z szerszych możliwości usługi chmurowej, zamierza rozszerzyć zakres usług o nowe funkcjonalności lub nowe procesy biznesowe lub o nowy zakres informacji przetwarzanych z wykorzystaniem usługi chmurowej. Nowa umowa z dostawca nie będzie zawierana, bo bank jako użytkownik narzędzia może z poziomu panelu administratora uruchamiać nowe usługi/przenosić kolejne procesy biznesowe/przetwarzać dodatkowe dane, bez konieczności zawierania nowej umowy/aneksowania dotychczasowej. Czy w takim przypadku bank powinien każdorazowo – rozszerzając sposób korzystania z narzędzia chmurowego o nowe usługi/funkcjonalności lub o kolejne procesy biznesowe lub przetwarzanie dodatkowych informacji - dokonywać notyfikacji do KNF?

XVII. Czy przepisy prawa dotyczące długości łańcucha outsourcingowego oraz Komunikat chmurowy w szczególności mają mieć zastosowanie, gdy istotą usługi zleconej przez bank swojemu usługodawcy nie jest przetwarzanie danych z wykorzystaniem przetwarzania w chmurze, ale do przetwarzania dochodzi „przy okazji" świadczenia usługi przez usługodawcę banku, w wyniku wykorzystywania przez usługodawcę typowych systemów i aplikacji chmury obliczeniowej,np.:

a) dostawca usług dla Banku przetwarza dane chronione z wykorzystaniem chmury publicznej, ale nie jest to outsourcing w rozumieniu prawa bankowego np. kancelaria prawna ma swoje systemy do w chmurze publiczne, swoje archiwa danych, kopie danych w chmurze publicznej;
b) kancelaria prawna udzielająca porad prawnych bankowi wykorzystuje w swojej codziennej działalności O365;
c) dostawca usług wspierających czynności windykacyjne (outsourcing w rozumieniu prawa bankowego) w bieżącej działalności spółki wykorzystuje O365, z wykorzystaniem tego narzędzia komunikuje się z bankiem, tworzy projekty pism do klientów itp.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

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

d) dostawca usług IT będący procesorem danych osobowych klientów banku (outsourcing w rozumieniu prawa bankowego) w bieżącej działalności wykorzystuje O365, np. komunikując się z bankiem, lub używając O365 do celów komunikacji wewnętrznej.

e) pośrednik kredytowy, skanuje dokumenty potencjalnego klienta, wprowadza dane kontaktowe potencjalnego klienta, a następnie przesyła je do banku z wykorzystaniem usług chmurowych np. poczty Microsoft albo Google. Pośrednik ten wykorzystuje te narzędzia na ogólnych zasadach, akceptując polityki i ogólne warunki tych dostawców.

Zwracamy przy tym uwagę, że literalne i mechaniczne zastosowanie przepisów dotyczących długości łańcucha outsourcingowego może oznaczać, że usługodawcy podmiotów nadzorowanych będą zmuszeni bądź do rezygnacji ze świadczenia usług na rzecz tych podmiotów, bądź do rezygnacji z rozwiązań chmurowych we własnej działalności lub wprowadzania równoległych systemów nie-chmurowych dla podmiotów nadzorowanych przez UKNF i chmurowych dla pozostałych podmiotów na rynku. Każda z tych sytuacji może podnieść w sposób znaczący koszty usług bez faktycznej zmiany ich jakości czy bezpieczeństwa danych.

XVIII. Stan faktyczny:

Podmiot nadzorowany nabywa oprogramowanie od dostawcy oprogramowania, który z kolei korzysta z usług innego dostawcy usługi chmurowej w zakresie IaaS lub PaaS, tzn. oprogramowanie „posadowione" jest na PaaS lub IaaS dostawcy usługi chmury obliczeniowej (sytuacja wskazana w pkt VI pkt 2 ppkt 7 Komunikatu). W oprogramowaniu przetwarzane są informacje prawnie chronione. Umowa pomiędzy dostawcą oprogramowania a dostawcą chmury zawarta jest na prawie państwa trzeciego tj. prawie stanu Waszyngton.

a) czy w związku z Cz VI pkt 2 ppkt 8) lit b) Komunikatu, podmiot nadzorowany powinien posiadać opinię, potwierdzającą, że zgodnie z prawem stanu Waszyngton wszystkie postanowienia umowy pomiędzy dostawcą oprogramowania a dostawcą usług chmury spełniają wymagania obowiązujące podmiot nadzorowany oraz wymagania Komunikatu? Jak powinna wyglądać taka opinia czy ma zawierać odniesienia do wszystkich punktów z Komunikatu – VI.2 pkt 8? Jaka konkluzja powinna wynikać z opinii, aby można było uznać, ze zastosowanie prawa państwa trzeciego nie generuje ryzyka?
b) czy w związku z Cz VI pkt 2 ppkt 8) lit b) Komunikatu, oraz mając na uwadze, że podmiot nadzorowany nie jest stroną umowy pomiędzy dostawcą oprogramowania a dostawcą chmury oraz nie jest w stanie uzyskać wglądu w taką umowę, taka opinia jest konieczna?
c) czy w związku z tym, iż dostawca oprogramowania nie jest w stanie udostępnić podmiotowi nadzorowanemu umowy z dostawcą chmurowym, w związku z czym podmiot nadzorowany nie może zlecić wykonania, taka opinia może być wykonana na zlecenie dostawcy chmurowego lub dostawcy oprogramowania i udostępniona podmiotowi nadzorowanemu i w ocenie UKNF, będzie traktowana jako opinia spełniająca warunek z Cz VI pkt 2 ppkt 8 Komunikatu?

XIX. W związku z Cz VI pkt 1 ppkt 8 lit a), w jaki sposób podmiot nadzorowany ma wykazać, że „prawo państwa trzeciego pozwala na skuteczne wykonywanie":

I. postanowień umowy;

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

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

II. wszystkich wymogów prawa polskiego ciążących na podmiocie nadzorowanym;
III. wytycznych organu nadzoru, w tym również w zakresie niniejszego komunikatu;

czy należy dołączyć opinię prawną w tym zakresie, a jeśli tak, to jakie dokładnie elementy powinny być uwzględnione w tej opinii?

XX. Które z wymagań z cz. VII pkt 4 (odnoszące się do dostawcy usługi chmury obliczeniowej) należy zawrzeć w umowie z dostawcą oprogramowania, w sytuacji gdy podmiot nadzorowany nie ma bezpośredniej relacji z dostawcą usług chmurowych, zaś dostawca usług chmury jest poddostawcą dostawcy oprogramowania?

XXI. *Podmiot nadzorowany nr 1 powierzył do przetwarzania informacje prawnie chronione w rozumieniu komunikatu chmurowego KNF podmiotowi nadzorowanemu nr 2, podmiot nadzorowany nr 2 korzysta do organizacji swojej pracy z oprogramowania do zarządzania projektami, treścią, kolejkami opracowanego przez dostawcę oprogramowania, które to oprogramowanie oparte jest o chmurę publiczną (narzędzie w modelu Software as a Service) i to dostawca oprogramowania ma umowę z dostawcą chmury publicznej:*

a. *czy podmiot nadzorowany nr 2 musi zawrzeć umowę uwzględniającą wszystkich uczestników łańcucha outsourcingowego (tj. podmiot nr 1, dostawcę oprogramowania, dostawcę chmury publicznej)?*
b. *czy w przypadku, gdy to podmiot nadzorowany nr 2 będzie szyfrował wysyłane dane prawnie chronione własnym sposobem (np. własny moduł HSM, własne zarządzanie kluczami) i spowoduje, że dostawca oprogramowania nie będzie miał faktycznego dostępu do danych prawnie chronionych, to czy oznacza to, że dostawca oprogramowania może być pominięty w ocenie dopuszczalności/długości łańcucha outsourcingowego? Czy wystarczy wtedy zawarcie np. umowy trójstronnej między podmiotem nr 1, podmiotem nr 2 i dostawcą chmurowym z pominięciem dostawcy oprogramowania?*

Jednocześnie wskazujemy, że jedną z najpoważniejszych barier dla clou computingu jest ograniczony łańcuch poddostawców (tak np. w outsourcingu bankowym, gdzie nadzorca dopuszcza łańcuch w postaci Bank-dostawca-poddostawca). Ponieważ usługi przetwarzania danych w chmurze mają zazwyczaj bardziej złożoną strukturę, konieczna jest zmiana systemowa. W najczęstszym modelu istnieje podmiot, który oferuje podmiotowi nadzorowanemu usługę (np. SaaS). Ten podmiot korzysta z platformy chmurowej (IaaS) jednego z dużych dostawców rozwiązań chmurowych. Te podmioty mają z kolei swoich poddostawców, choćby spółki celowe posiadające i zarządzające centrami przetwarzania danych (listy poddostawców operatorów rozwiązań chmurowych można znaleźć na stronach internetowych tych dostawców).

XXII. Klucze szyfrujące a Komunikat

1. Komunikat w swojej nomenklaturze operuje różnorodnymi pojęciami odnoszącymi się do **kluczy szyfrujących**, w zależności od szczegółowego przedmiotu regulacji zawartego w Komunikacie, tj. w szczególności:
   a) „posiadanie dostępu do kluczy szyfrujących” (pkt. I. 1. 23),

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

b) „zarządzanie kluczami szyfrującymi" (m.in. pkt. VI. 1. 5) a), f), pkt. VI. 1. 6) b) i., pkt. VI 5.1 b), pkt. VII 5. b),
c) „generowanie kluczy szyfrujących" (m.in. pkt. VII 7.2),
d) „dostarczenie kluczy szyfrujących" (m.in. pkt. VI 2.6 b) i.),
e) „przechowywanie kluczy szyfrujących" (pkt. VII 7.5).

2. Zgodnie ze stanowiskiem UKNF, jeżeli dostawca usług chmury obliczeniowej (lub jego poddostawca) **posiada lub może posiadać dostęp do kluczy szyfrujących**, jest to wystarczające do uznania, że zachodzi „ujawnienie informacji" przetwarzanych w chmurze obliczeniowej, nawet gdyby zachodziło szyfrowanie takich informacji „at rest" lub „in transit" (co wynika z definicji zawartej w pkt. I.1. 23).

3. W dalszej treści Komunikatu, UKNF większą uwagę poświęca zagadnieniu „zarządzania kluczami szyfrującymi"; m.in. zgodnie ze stanowiskiem wyrażonym w pkt. VI. 2. 5) b) i f), *(…) szyfrowanie informacji oraz* ***właściwe zarządzanie kluczami szyfrującymi zapobiega ujawnieniu informacji****; (…) Nadzór dopuszcza sytuację, w której podmiot nadzorowany powierza swojemu dostawcy usług (w tym dostawcy usług chmury obliczeniowej)* ***generowanie lub zarządzanie kluczami szyfrującymi, które są używane do szyfrowania informacji przetwarzanej w usługach chmury obliczeniowej innego dostawcy usług chmury obliczeniowej****, przy czym podmiot nadzorowany powinien w procesie szacowania ryzyka uwzględnić możliwość* ***utraty swojego dostępu do kluczy szyfrujących****;*

4. Zgodnie z pkt. VI. 2. 6) b) i., *(…) zakres odpowiedzialności dostawcy usług chmury obliczeniowej oraz jego poddostawców wobec podmiotu nadzorowanego może ulegać ograniczeniu albo wyłączeniu wyłącznie w granicach szczególnych przepisów prawa regulujących działalność podmiotu nadzorowanego, przy czym Nadzór krytycznie ocenia takie wyłączenia albo ograniczenia, jeżeli:*

i. w ramach usługi chmury obliczeniowej przetwarzane są informacje prawnie chronione ***szyfrowane za pomocą kluczy szyfrujących dostarczonych lub zarządzanych przez dostawcę usług chmury obliczeniowej lub jego poddostawcę*** *(…).*

5. Zgodnie z pkt. VII. 7.2, *Podmiot nadzorowany powinien zapewnić, że informacje są szyfrowane kluczami* ***generowanymi oraz zarządzanymi przez podmiot nadzorowany, chyba że z oszacowania ryzyka wynika, iż dopuszczalne lub wskazane jest używanie kluczy szyfrujących generowanych lub zarządzanych przez dostawcę usług chmury obliczeniowej.***

Na rynku usług chmurowych dostępne są różnorodne rozwiązania zmierzające do zapewnienia kontroli klienta nad kluczami szyfrującymi (i zarazem zapobiegające możliwości dostępu do danych klienta), przy jednoczesnym braku utraty podstawowych funkcjonalności związanych z usługą chmurową.
Wobec różnorodności pojęć związanych z kluczami szyfrującymi, którymi operuje Komunikat, mogą nasuwać się wątpliwości, czy niektóre rozwiązania dostępne na rynku, zgodne są z intencjami UKNF w zakresie podejścia do kluczy szyfrujących, a które znalazły odzwierciedlenie w wymogach Komunikatu.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

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

Pytania dot. kluczy szyfrujących

Pytanie: Czy przez posiadanie (lub możliwość posiadania) dostępu do kluczy szyfrujących przez dostawcę usług chmury obliczeniowej lub jego poddostawcę (zgodnie z definicją zawartą w pkt. I.1.23) Komunikatu) należy rozumieć również sytuację, w której, wprawdzie klucze szyfrujące są przechowywane w infrastrukturze dostawcy usług chmury obliczeniowej lub jego poddostawcy, lecz to podmiot nadzorowany generuje, dostarcza i zarządza takimi kluczami szyfrującymi ?

Odpowiedź na to pytanie ma szczególne znaczenie w kontekście definicji „ujawnienia informacji". W kontekście dalszych zapisów Komunikatu można wysnuć wniosek, że w przypadku generowania, dostarczania oraz zarządzania kluczami szyfrującymi przez podmiot nadzorowany (niezależnie od miejsca ich przechowywania), to podmiot nadzorowany powinien być traktowany jako ten, który posiada dostęp do kluczy szyfrujących w rozumieniu ww. definicji, a z drugiej strony w takim wypadku dostawca usług chmury obliczeniowej nie posiada dostępu do kluczy ani nie ma takiej możliwości, a w związku z tym sam fakt przechowywania kluczy w infrastrukturze dostawcy nie przesądza o ujawnieniu informacji (gdyż kluczowe są elementy generowania, dostarczania i zarządzania kluczami).

1. **Pytanie: Czy wskazane w pkt. I. 1 nin. wiadomości, pojęcia „generowania" i „dostarczania" kluczy szyfrujących, są tożsame?**

Odpowiedź na to pytanie pozwoli usunąć stan niejednoznaczności, wobec stosowania w Komunikacie różnych pojęć odnoszących się, jak się wydaje, do takich samych (lub podobnych) sytuacji. W naszej ocenie ww. pojęcia są zbieżne.

2. **Pytanie: Jakie elementy (czynności) wchodzą w skład zarządzania kluczami szyfrującymi w rozumieniu Komunikatu?**

Odpowiedź na to pytanie pozwoli doprecyzować ww. pojęcie i uniknąć niejednoznaczności, zwłaszcza wobec braku definicji zarządzania kluczami szyfrującymi w Komunikacie, jak i odrębnego stosowania różnych pojęć odnoszących się do kluczy szyfrujących, jak wskazano już wyżej, m.in. posiadanie dostępu, przechowywanie, generowanie, dostarczanie.

4. **Pytanie: Czy jeśli podmiot nadzorowany, w ramach infrastruktury tego samego dostawcy usług chmury obliczeniowej, w jednym tenancie korzysta z „właściwych" usług chmury obliczeniowej, a w ramach innego tenanta przechowuje i zarządza kluczami szyfrującymi (wygenerowanymi przez siebie), to czy w takim modelu można uznać, że w stosunku do dostawcy (ewent. poddostawcy) nie zachodzi ujawnienie informacji w rozumieniu Komunikatu?**

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

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

Wskazany wyżej model zakłada zarządzanie kluczami szyfrującymi przez podmiot nadzorowany, jednak z uwzględnieniem rozdzielenia tenanta dla usługi od tenanta dla zarządzania kluczami. Rozdzielenie tenantów stanowi dodatkowe wzmocnienie w procesie zarządzania kluczami szyfrującymi przez podmiot nadzorowany i powinno potwierdzać, że nie zachodzi ujawnienie informacji.

5. **Pytanie: Czy jeśli podmiot nadzorowany, zgodnie z pkt. VI. 2. 5) f) Komunikatu, powierza generowanie lub zarządzanie kluczami szyfrującymi innemu dostawcy usług chmury obliczeniowej (dostawca nr 1), aniżeli dostawcy usług chmury obliczeniowej, w którego chmurze są przetwarzane informacje podmiotu nadzorowanego podlegające szyfrowaniu (dostawca nr 2), to czy:**
   a) **w świetle wymogu zawartego w pkt. VII 7.2, jest to równoznaczne z sytuacją, w której to sam podmiot nadzorowany generuje i zarządza kluczami szyfrującymi?**
   b) **jest to wystarczające do uznania, że w stosunku do któregokolwiek z ww. dostawców (nr 1 lub 2) nie zachodzi ujawnienie informacji w rozumieniu Komunikatu?**

W omawianych przypadkach można założyć, że dostawca nr 1 nie ma dostępu do szyfrowanych informacji, a dostawca nr 2 nie posiada dostępu do kluczy szyfrujących, co uzasadniałoby odpowiedzi twierdzące na zadane pytania.

XXIII. Informowanie UKNF o outsourcingu chmury obliczeniowej w razie zmian dokonywanych w dokumentacji wymaganej Komunikatem.

1. Podmiot nadzorowany informuje UKNF o outsourcingu chmury obliczeniowej na zasadach wskazanych w pkt. VIII ppkt. 1 i 2 Komunikatu.
2. Zważywszy na zakres informacji przekazywanych UKNF w zw. z outsourcingiem chmury obliczeniowej:

Pytanie: Czy UKNF zaleca, by w przypadku wystąpienia istotnych zmian w rodzaju i zakresie informacji planowanych do przetwarzania / przetwarzanych w chmurze obliczeniowej (o których podmiot nadzorowany informuje UKNF na podstawie pkt. VIII ppkt. 1.1), w stosunku do rodzaju i zakresu informacji, które już wcześniej zostały zgłoszone w ramach poinformowania UKNF na podstawie pkt. VIII ppkt. 1 i 2 Komunikatu (i w ramach tego samego outsourcingu chmury obliczeniowej), by podmiot nadzorowany ponownie poinformował UKNF o outsourcingu chmury obliczeniowej, aktualizując treść ww. zgłoszenia?

Pytanie w praktyce odnosi się np. do sytuacji, w której podmiot nadzorowany przetwarza w chmurze obliczeniowej „okrojony" zakres informacji prawnie chronionych w ramach tzw. rozwiązania pilotażowego, a następnie planuje znacząco rozszerzyć rodzaj i zakres informacji przetwarzanych w chmurze w ramach tzw. rozwiązania produkcyjnego (np. w zakresie korzystania z tej samej aplikacji SaaS lub środowiska IaaS).

XXIV. Testowanie exit planu – pytanie doprecyzowujące

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

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

1. Zgodnie ze stanowiskiem UKNF wyrażonym w Q&A na stronie https://www.knf.gov.pl/dla_rynku/fin_tech/chmura_obliczeniowa/Q&A w odpowiedzi na zagadnienie: *Plan wycofania i przeprowadzenie testów wycofania. VII.5.3. Komunikatu. /data publikacji 25-03-2021/,* UKNF stanął na stanowisku, że:

Podmiot nadzorowany powinien zidentyfikować, z jakich procesów i aplikacji korzysta. Następnie podmiot nadzorowany powinien zbadać, w szczególności z uwzględnieniem VI.2.1.e i h Komunikatu, które z tych procesów i aplikacji mają ***istotny wpływ na działalność podmiotu nadzorowanego (tzn. ich brak działania lub działanie nieprawidłowe istotnie wpłynie na funkcjonowanie podmiotu nadzorowanego z perspektywy skutków ekonomicznych, skutków dla reputacji podmiotu nadzorowanego, skutków dla klientów podmiotu nadzorowanego oraz wymogów nadzorczych związanych z prowadzoną przez niego działalnością), oraz które procesy i aplikacje mogą zostać przeniesione do innych dostawców usługi chmury obliczeniowej lub do infrastruktury on premise.***

Kwalifikacja, czy dany proces i aplikacja ma istotne znaczenie ***odbywa się w oparciu o szacowanie ryzyka.*** *Szacowanie ryzyka jest przeprowadzane samodzielnie przez podmiot nadzorowany. UKNF dopuszcza wykorzystanie do szacowania ryzyka standardów opracowanych w ramach zrzeszeń branżowych lub innych powszechnie przyjętych.*

Testowanie planu wycofania dotyczy procesów i aplikacji, a nie dostawcy usługi chmury obliczeniowej. Testowanie nie może ograniczać się jedynie do teoretycznych ćwiczeń symulujących podjęcie adekwatnych kroków w przypadku wystąpienia określonych zdarzeń (przeprowadzenie gry sztabowej). Testowanie powinno odbywać się przynajmniej raz w roku ***poprzez rzeczywiste wykonanie działań awaryjnych w stosunku do procesów i aplikacji, które mają istotny wpływ na działalność podmiotu nadzorowanego.***

2. Zważywszy na powyższe wyjaśnienia:

Pytania:

a) Czy w zakresie procesów/aplikacji, z uwagi na które podmiot nadzorowany dokonał kwalifikacji outsourcingu chmury obliczeniowej jako outsourcing szczególny chmury obliczeniowej w rozumieniu Komunikatu, UKNF dopuszcza sytuację, w której dany proces realizowany w chmurze (lub aplikacja chmurowa) nie nosi jednak znamion istotnego (istotnej) w rozumieniu wyjaśnienia z pkt. 1 powyżej?

b) Czy można dopuścić sytuację odwrotną, tj. czy jeśli podmiot nadzorowany nie zakwalifikował outsourcingu chmury obliczeniowej jako outsourcingu szczególnego chmury obliczeniowej w rozumieniu Komunikatu, to czy podmiot nadzorowany może automatycznie założyć, że dany proces realizowany w chmurze (lub aplikacja chmurowa) nie nosi znamion istotnego (istotnej) w rozumieniu wyjaśnienia z pkt. 1 powyżej?

Z uwagi na specyfikę exit planu, należy założyć, że nie każdy outsourcing szczególny będzie oznaczał konieczność uznania danego procesu/aplikacji za istotne w rozumieniu wyjaśnienia z pkt. 1 (pytanie z lit. a), natomiast z drugiej strony należy założyć, że brak uznania procesu/aplikacji za outsourcing szczególny, daje podstawy do uznania, że dany proces/aplikacja nie nosi znamion istotnej w rozumieniu wyjaśnienia z pkt. 1 powyżej.