MODEL WDROŻENIA USŁUGI CHMURY OBLICZENIOWEJ

IZFIA

Warszawa, 2023 r.

Izba Zarządzających Funduszami i Aktywami

SPIS TREŚCI

1. AUTORZY MODELU

Model wdrożeń w chmurze obliczeniowej publicznej lub hybrydowej został opracowany w ramach prac grupy roboczej powołanej przy Izbie Zarządzających Funduszami i Aktywami.

KOORDYNATORZY PROJEKTU:

Magdalena Chodkiewicz, Izba Zarządzających Funduszami i Aktywami

Szymon Ciach, Kochański & Partners

ZESPÓŁ REDAKCYJNY:

Krzysztof Kowacz, Kochański & Partners
Maciej Kuranc, Kochański & Partners
Sylwia Magott, Noble Funds TFI
Agnieszka Ulanowska, Noble Funds TFI
Bartłomiej Kaja, Noble Funds TFI
Monika Łasiewicka, Rockbridge TFI
Dominik Mielczarek, Pekao TFI
Justyna Sokół, Pekao TFI
Krzysztof Turek, PKO BP Finat
Barbara Liszewska, PKO BP Finat
Rafał Syska, Investors TFI
Łukasz Lenarczyk, Millennium TFI
Łukasz Wantola, Millennium TFI
Anna Rzeszutek, IPOPEMA TFI
Dariusz Korona, NN Investment Partners TFI
Anna Łukaszewicz, ProService Finteco
Michał Cichocki, Noble Funds TFI
Piotr Wiejak, Rockbridge TFI
Maciej Kujawa, Rockbridge TFI
Dariusz Siewiera, TFI PZU
Artur Fajok, ProService Finteco
Artur J. Kępa, ProService Finteco
Tadeusz Skrodzki, PFR TFI
Leszek Wałach, NN Investment Partners TFI
Kamila Chojnowska, Pekao TFI
Tomasz Szurek, BEST TFI
Michał Majewski, Intrum TFI
Bartłomiej Erchardt, Rockbridge TFI
Krzysztof Andrzejczyk, TFI PZU
Sylwia Ziółkiewicz, UNIQA TFI
Paweł Ornoch, PKO BP Finat
Tomasz Szymański, Investors TFI
Karol Waliszewski, BEST TFI

Łukasz Balcerzak, Investors TFI
Mariola Bargielska, BEST TFI
Magdalena Wachowska, BEST TFI
Krzysztof Maderak, PKO TFI
Katarzyna Serafińczyk-Skorupka, UNIQA TFI
Adrian Panek, PKO BP Finat
Maciej Jurczyk, PKO BP Finat
Piotr Patroński, PKO BP Finat
Ewelina Subda, PKO BP Finat
Bartosz Błaszak, BEST TFI
Magdalena Rosinke, BEST TFI
Oskar Janiszek, IPOPEMA TFI
Ireneusz Skowroński, Esaliens TFI
Robert Strupiechowski, Investors TFI
Łukasz Adaś, NN Investment Partners TFI

2. WSTĘP

ODPOWIEDŹ NA POTRZEBY RYNKU

Wychodząc naprzeciw oczekiwaniom rynkowym Funduszy Inwestycyjnych oraz zarządzających Alternatywnymi Funduszami Inwestycyjnymi w zakresie możliwości wdrażania rozwiązań opartych o usługi chmury obliczeniowej w wybranych podmiotach objętych nadzorem nad rynkiem kapitałowym, Izba Zarządzających Funduszami i Aktywami powołała do życia grupę roboczą, której celem jest ułatwienie uczestnikom tego sektora przeprowadzenie skutecznego i bezpiecznego procesu transformacji cyfrowej.

Działalność polegająca na zarządzaniu Funduszami Inwestycyjnymi i obr aktywami w Polsce uregulowana jest w treściach ustaw, rozporządzeń oraz rekomendacji i wytycznych nadzoru finansowego regulujących jej ramy. Stworzenie kompleksowego i praktycznego przewodnika dla sektora inwestycyjnego nie jest zadaniem łatwym. Zainteresowanie branży, przy jednocześnie niewielkiej praktyce Funduszy Inwestycyjnych i zarządzających Alternatywnymi Funduszami Inwestycyjnymi w zakresie wykorzystania usług chmurowych, skłoniło autorów niniejszego opracowania do stworzenia wspólnej inicjatywy, w celu przygotowania modelu wdrożenia rozwiązań informatycznych opartych o chmurę obliczeniową w tych podmiotach.

W październiku 2017 r. Urząd Komisji Nadzoru Finansowego opublikował komunikat dotyczący korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej.

W dniu 24 stycznia 2020 r. Urząd Komisji Nadzoru Finansowego opublikował kolejny komunikat, dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej (Komunikat). Komunikat, zgodnie z jego brzmieniem, uzupełnia i uszczegóławia wybrane zalecenia w zakresie outsourcingu, opisane między innymi w ustawie o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi. Regulacje te nie mogą być pominięte przy określaniu możliwości, a następnie przy faktycznym wdrożeniu rozwiązań opartych o chmurę obliczeniową.

Przy aktywnym udziale sektora inwestycyjnego, wykorzystując dotychczasowe doświadczenia, płynące z przeprowadzanych już wdrożeń, postanowiliśmy przeanalizować postanowienia Komunikatu i w szerokim gronie wypracować wspólnie model, stanowiący możliwie kompleksowy zbiór praktyk i rozwiązań umożliwiających Funduszom Inwestycyjnym oraz podmiotom zarządzającym Alternatywnymi Funduszami Inwestycyjnymi proste przejście przez proces adaptacji do chmury obliczeniowej, zarówno w przypadku całej organizacji, jak i wyłącznie w zakresie wybranych rozwiązań oferowanych przez dostawców usług chmurowych.

Niniejszy Model prezentuje, jakie zadania, procedury, procesy i analizy fundusz inwestycyjny lub podmiot zarządzający alternatywnym funduszem inwestycyjnym powinien przeprowadzić i udokumentować, aby poprawnie przygotować organizację do działania w sferze usług chmurowych w odniesieniu do poszczególnych zapisów wybranych regulacji.

MATERIAŁY ŹRÓDŁOWE

Niniejszy dokument wraz z załącznikami został stworzony przy wykorzystaniu materiałów bankowego standardu wdrożenia usługi chmury obliczeniowej publicznej lub hybrydowej „PolishCloud 2.0.", opracowanego przez grupę roboczą powołaną przy Forum Technologii Bankowych ZBP i Radzie Bankowości Elektronicznej ZBP. W tym miejscu chcielibyśmy podziękować Związkowi Banków Polskich za wyrażenie zgody na wykorzystanie materiału i dorobku środowiska bankowego.

Standard PolishCloud 2.0. dostępny jest pod adresem: https://zbp.pl/Dla-Bankow/Bankowosc-elektroniczna/PolishCloud

ZAŁOŻENIA

Podkreślenia wymaga, iż niniejszy Model odnosi się do wymogów dotyczących korzystania z rozwiązań chmurowych przez wybrane podmioty objęte nadzorem nad rynkami kapitałowymi w rozumieniu Ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (tj. Dz. U. z 2020 r. poz. 180, ze zmianami), wskazane w definicji Podmiotów nadzorowanych przyjętej w Modelu. Model nie odnosi się zatem do wymogów dotyczących rozwiązań chmurowych dla podmiot w objętych innym nadzorem wskazanym w tej ustawie.

Zasadniczą podstawą Modelu są wymogi komunikatu UKNF z dnia 24 stycznia 2020 r., a co za tym idzie, przedstawia on wymagania w przypadku przetwarzania w Podmiotach nadzorowanych (zgodnie z definicją) informacji w chmurze obliczeniowej publicznej lub chmurze obliczeniowej hybrydowej.

STOSOWANIE MODELU

Model może być wykorzystany jako przykładowy sposób postępowania przez podmioty sektora inwestycyjnego w planowanych wdrożeniach chmurowych. Jego stosowanie natomiast każdorazowo powinno uwzględniać specyfikę działalności danego podmiotu nadzorowanego.

W przypadku wątpliwości w zakresie zastosowania Modelu w swojej działalności, Podmiot nadzorowany ma możliwość zwrócenia się do UKNF w celu wyjaśnienia danego problemu w kontekście określonego stanu faktycznego.

Niniejszy Model może być również wykorzystywany przez inne podmioty niż podmioty sektora funduszy inwestycyjnych, jednak w takiej sytuacji powinny one uwzględnić, że część zagadnień, zwłaszcza ściśle związanych z kwestiami prawnymi, jest specyficzna wyłącznie dla sektora rynku kapitałowego w zakresie działalności prowadzonej przez Podmioty nadzorowane.

WSPÓŁPRACA

IZFiA zachęca podmioty korzystające z Modelu do dzielenia się swoimi spostrzeżeniami, doświadczeniami i opiniami w zakresie jego stosowania poprzez kontakt na adres mailowy: poczta@izfa.pl.

Oceny i przemyślenia osób korzystających z Modelu umożliwią jego dalsze usprawnianie, które odbywać się będzie poprzez jego aktualizowanie i dalsze dostosowywanie do potrzeb rynku i jego uczestników. Ponadto, pozwolą autorom zidentyfikować najważniejsze problemy i ewentualnie skierować odpowiednie pytania do UKNF w celu ich wyjaśnienia i rozwiązania.

Żywimy nadzieję, że niniejszy Model okaże się dla użytkowników przydatnym narzędziem i stanowić będzie praktyczny przewodnik po meandrach procesu wdrażania chmury obliczeniowej w Podmiotach nadzorowanych.

Autorzy

3. TERMINOLOGIA STOSOWANA W MODELU

W niniejszym Modelu zasadniczo przyjęto terminologię stosowaną w Komunikacie, z uwzględnieniem komentarzy zamieszczonych poniżej.

DEFINICJE Z KOMUNIKATU	ZNACZENIE PRZYJĘTE W MODELU
Chmura obliczeniowa	Zgodnie ze znaczeniem nadanym w Komunikacie, jest to 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. Na potrzeby Modelu, przez Chmurę obliczeniową rozumiemy Chmurę obliczeniową publiczną i Chmurę obliczeniową hybrydową.
Chmura obliczeniowa hybrydowa	Zgodnie ze znaczeniem nadanym w Komunikacie jest to chmura obliczeniowa składająca się z połączenia dwóch lub więcej osobnych chmur obliczeniowych (publicznej, prywatnej, społecznościowej), która poprzez standaryzację użycia lub odpowiednią technologię pozwala na przenoszenie czynności przetwarzania informacji pomiędzy chmurami obliczeniowymi, które ją tworzą.
Chmura obliczeniowa publiczna	Zgodnie ze znaczeniem nadanym w Komunikacie jest to chmura obliczeniowa dostępna do użytku publicznego, będąca w posiadaniu lub bezpośrednio zarządzana przez dostawcę usług chmury obliczeniowej.
Chmura obliczeniowa prywatna	Zgodnie ze znaczeniem nadanym w Komunikacie, jest to chmura obliczeniowa dostępna do wyłącznego użytku jednego podmiotu, będąca w posiadaniu lub bezpośrednio zarządzana przez ten podmiot. Jako chmurę prywatną w szczególności można traktować infrastrukturę serwerowo-storage'ową (wraz z dedykowanym wdrożeniem oprogramowania zarządzającego chmurą), dedykowaną dla podmiotu nadzorowanego, przy jednoczesnym korzystaniu ze współdzielonych fizycznie zasobów infrastruktury sieciowej. Korzystanie z takich zasobów sieciowych nie zmienia kwalifikacji chmury jako prywatnej.
Chmura obliczeniowa społecznościowa	Zgodnie ze znaczeniem nadanym w Komunikacie jest to chmura obliczeniowa dostępna do wyłącznego użytku grupy podmiotów powiązanych kapitałowo lub na mocy wspólnej umowy o współpracy, ze zdefiniowanymi wspólnymi wymaganiami i zasadami, m.in. w obszarze zgodności i bezpieczeństwa przetwarzania informacji, będąca w posiadaniu lub bezpośrednio zarządzana przez podmiot(y) z grupy lub na jego (ich) zlecenie. Chmura obliczeniowa społecznościowa może mieć zarówno charakter:

	1. chmury obliczeniowej prywatnej, gdy jest dostępna do wyłącznego użytku grupy podmiotów powiązanych kapitałowo lub na mocy wspólnej umowy i jest przy tym zarządzana przez podmiot z grupy, albo 2. chmury obliczeniowej publicznej, gdy jest dostępna do wyłącznego użytku grupy podmiotów powiązanych kapitałowo lub na mocy wspólnej umowy, lecz jest przy tym zarządzana przez Dostawcę.
CPD	Zgodnie ze znaczeniem nadanym w Komunikacie – centrum przetwarzania danych.
Dostawca usług chmury obliczeniowej	Zgodnie ze znaczeniem nadanym w Komunikacie jest to podmiot, który dysponuje infrastrukturą i oprogramowaniem służącym do świadczenia usług chmury obliczeniowej oraz świadczy usługi chmury obliczeniowej. W kontekście usług SaaS, Dostawcą usług chmury obliczeniowej jest dostawca SaaS, o ile bierze na siebie odpowiedzialność wobec klienta za cały stos technologiczny dostarczanego rozwiązania (odpowiada za aplikację oraz jej hosting, nawet jeśli w zakresie hostingu korzysta z poddostawcy).
EOG	Europejski Obszar Gospodarczy.
Informacja prawnie chroniona	Zgodnie ze znaczeniem nadanym w Komunikacie oznacza informację związaną z tajemnicami sektora finansowego, wymienionymi w ustawach sektorowych. Przez informacje prawnie chronione rozumie się Tajemnicę zawodową.
Model	Oznacza niniejsze opracowanie.
KNF	Komisja Nadzoru Finansowego.
Kodeks cywilny	Oznacza ustawę z dnia 23 kwietnia 1964 r. – Kodeks cywilny (tj. Dz. U. z 2019 r. poz. 1145, ze zmianami).
Komunikat	Komunikat Urzędu Komisji Nadzoru Finansowego z dnia 23 stycznia 2020 r., dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej.

Łańcuch outsourcingowy	Zgodnie ze znaczeniem nadanym w Komunikacie oznacza relację polegającą na: 1) powierzeniu przez Dostawcę usług chmury obliczeniowej części czynności (służących dostarczaniu usługi chmury obliczeniowej dla podmiotu nadzorowanego) swojemu poddostawcy i dalszym (kolejnym) poddostawcom lub 2) dostarczaniu przez Dostawcę usług chmury obliczeniowej usługi chmury obliczeniowej innemu dostawcy, który wykorzystuje usługę chmury obliczeniowej do świadczenia własnej usługi dla podmiotu nadzorowanego.
Outsourcing chmury obliczeniowej	Zgodnie ze znaczeniem nadanym w Komunikacie, oznacza umowę zawartą w dowolnej formie między podmiotem nadzorowanym, a dostawcą usług chmury obliczeniowej, na mocy której Dostawca usług chmury obliczeniowej, dostarcza podmiotowi nadzorowanemu usługę chmury obliczeniowej, która służy do wsparcia realizacji procesu, usługi lub zadania, które podmiot nadzorowany realizowałby samodzielnie, gdyby usługa chmury obliczeniowej była niedostępna.
Outsourcing regulowany	Powierzenie czynności o którym mowa w art. 45a ust. 1 (outsourcing TFI) lub art. 70g ust. 1 (outsourcing ASI) UFI.
Outsourcing szczególny chmury obliczeniowej lub Outsourcing szczególny	Zgodnie ze znaczeniem nadanym w Komunikacie, 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: 1) wpływałaby w sposób istotny na ciągłość wypełniania przez podmiot nadzorowany warunków stanowiących podstawę uprawnienia prowadzenia działalności nadzorowanej lub jej wykonywania, lub 2) zagrażałoby w sposób istotny wynikom finansowym podmiotu nadzorowanego, niezawodności lub ciągłości wykonywania działalności nadzorowanej. Dodatkowo, zgodnie z Q&A chmurowym, Podmiot nadzorowany w kontekście kwalifikacji danej czynności lub funkcji jako outsourcingu szczególnego chmury obliczeniowej, powinien przy takiej kwalifikacji brać pod uwagę skalę ocenianego procesu (czynności lub funkcji) i fakt, że może ona się zmieniać w trakcie prowadzonej działalności. Jak wskazuje UKNF: „proces, który wyjściowo nie był oceniany jako krytyczny i istotny, może z biegiem czasu zwiększyć swoją skalę i przez to powinien zostać zakwalifikowany jako kluczowy i krytyczny”.

Poddostawca	Zgodnie ze znaczeniem nadanym w Komunikacie jest to podmiot, który świadczy usługi dla dostawcy usług chmury obliczeniowej, służące dostarczaniu usługi chmury obliczeniowej dla podmiotu nadzorowanego i posiada albo może posiadać identyfikowany dostęp do informacji przetwarzanych przez podmiot nadzorowany. Poddostawcą, w rozumieniu Komunikatu jest podmiot, który: 1) świadczy usługi dla dostawcy usług chmury obliczeniowej, służące dostarczaniu usługi chmury obliczeniowej dla Podmiotu nadzorowanego, oraz 2) posiada lub może posiadać identyfikowany dostęp do informacji przetwarzanych przez Podmiot nadzorowany. W kontekście Komunikatu dochodzi do zawężenia zakresu znaczenia „poddostawców" do podmiotów, które świadczą na rzecz dostawcy usług chmurowych tego typu usługi, które są bezpośrednio i funkcjonalnie związane z możliwością świadczenia usługi chmurowej. Przykłady: Poddostawcą będzie podmiot będący poddostawcą Dostawcy, prowadzący działalność centrum hostingowego (chmury w ścisłym tego słowa znaczeniu), w którym będzie zainstalowane i eksploatowane oprogramowanie, oferowane Podmiotowi nadzorowanemu łącznie z usługą dostawy mocy obliczeniowej w ramach tego centrum. Nie będzie poddostawcą jednak np. kontrahent centrum hostingowego odpowiadający za utrzymanie czystości, agencja ochrony mienia, a nawet wynajmujący - właściciel budynku. Przez identyfikowany dostęp do informacji przetwarzanych przez Podmiot nadzorowany rozumieć należy taki dostęp, który spełnia następujące kryteria: 1) umożliwia poddostawcy identyfikację Podmiotu nadzorowanego jako zleceniodawcy, 2) dochodzi do ujawnienia przetwarzanych danych (informacji) w rozumieniu nadanym przez Komunikat, przy czym to zapisy kontraktowe lub sposób skonfigurowania szyfrowania informacji powinny decydować o tym, czy podmiot posiada i w jaki sposób może uzyskać posiadanie takiego identyfikowanego dostępu (np. gdy technicznie możliwy jest dostęp, natomiast umowa zakazuje wykorzystywania takiej możliwości).

	Dodatkowo wskazać należy, że poddostawcą będzie firma współpracująca z Dostawcą, która ma logiczny, a nie fizyczny, dostęp do informacji przetwarzanych przez Podmiot nadzorowany.
Podmiot nadzorowany	Podmiot nadzorowany w rozumieniu Komunikatu. Na potrzeby Modelu przez Podmioty nadzorowane rozumie się poniższe podmioty zgodnie z definicjami zawartymi w UFI: 1) Towarzystwo funduszy inwestycyjnych; 2) Zarządzający alternatywną spółką inwestycyjną; 3) Fundusz inwestycyjny.
RODO	Oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
Tajemnica zawodowa	Oznacza tajemnicę zawodową opisaną w art. 280 ust. 2 UFI oraz w art. 147 Ustawy o obrocie.
Udokumentowany proces	Zgodnie ze znaczeniem nadanym w Komunikacie oznacza zbiór powiązanych ze sobą, systematycznie realizowanych czynności, które są stosowane i wystarczająco szczegółowo dla podmiotu nadzorowanego opisane w dokumentach zewnętrznych lub wewnętrznych, wyniki tych czynności są zapisywane, a zapisy przechowywane w sposób pozwalający na wykazanie wykonania czynności zgodnie z wymaganiami.
Ujawnienie informacji	Zgodnie ze znaczeniem nadanym w Komunikacie oznacza sytuację, podczas której informacje są przetwarzane w chmurze obliczeniowej: 1) w sposób nieszyfrowany albo 2) w sposób zaszyfrowany „at rest" lub „in transit", ale dostęp do kluczy szyfrujących i szyfrowanej tymi kluczami informacji posiada albo może posiadać dostawca usług chmury obliczeniowej lub jego poddostawca w łańcuchu outsourcingowym.
UKNF	Urząd Komisji Nadzoru Finansowego.

Umowa Nieistotna	Umowa, o której mowa w art. 45a. ust. 8 UFI, tj. umowa, której 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 UFI.
Usługa chmury obliczeniowej	Zgodnie ze znaczeniem nadanym w Komunikacie oznacza gotowe do użycia, wystandaryzowane zasoby chmury obliczeniowej służące przetwarzaniu informacji, wstępnie skonfigurowane przez dostawcę usług chmury obliczeniowej i przez niego dostarczane; mogą być bezpośrednio dostarczane podmiotowi nadzorowanemu lub stanowić element usług innego dostawcy na różnym poziomie łańcucha outsourcingowego.
UFI	Oznacza ustawę z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi, ze zmianami.
Ustawa o nadzorze nad rynkiem finansowym	Oznacza ustawę z dnia 21 lipca 2006 r., o nadzorze nad rynkiem finansowym, ze zmianami.
Ustawa o obrocie	Oznacza ustawę z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, ze zmianami.
Wartość informacji	Zgodnie ze znaczeniem nadanym w Komunikacie oznacza konsekwencję dla działalności podmiotu nadzorowanego materializacji ryzyka polegającego na nieuprawnionym ujawnieniu, zmianie lub zniszczeniu informacji.
Wytyczne ESMA	Wytyczne Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych z 10 maja 2021 roku dotyczące outsourcingu do dostawców usług chmury.
Zasada proporcjonalności	Wyłącznie pomocniczo, zamieszczamy wyjaśnienie zasady proporcjonalności, którego brak w Komunikacie. Zgodnie z Wytycznymi Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych z 10 maja 2021 roku dotyczące outsourcingu do dostawców usług chmury, firmy w myśl zasady proporcjonalności, powinny uwzględniać charakter, skalę i złożoność funkcji, którą firma zamierza zlecić na zasadzie outsourcingu oraz do ryzyka nieodłącznie związanego z tą funkcją. Zgodnie z Wytycznymi UKNF dotyczącymi zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w towarzystwach funduszy inwestycyjnych z 16 grudnia 2014 r.(„**Wytyczne**”) zasada proporcjonalności przejawia się w tym, że przy uwzględnianiu specyfiki zagadnień związanych z technologią i bezpieczeństwem środowiska teleinformatycznego oraz różnic w zakresie uwarunkowań, skali działalności oraz profili ryzyka towarzystw funduszy inwestycyjnych, sposób realizacji zaleceń Komunikatu może być i wskazanych w nim celów może być odmienny. Oznacza to, że stosowanie tych praktyk powinno zależeć m.in. od tego, na ile przystają one do specyfiki i profilu ryzyka towarzystwa funduszy inwestycyjnych, szczególnych uwarunkowań prawnych, w jakich towarzystwo funduszy inwestycyjnych się znajduje oraz charakterystyki jego środowiska teleinformatycznego, jak również od stosunku kosztów ich wprowadzenia do

	wynikających z tego korzyści (także z perspektywy bezpieczeństwa klientów towarzystwa funduszy inwestycyjnych). Zgodnie ze stanowiskiem wyrażonym w Wytycznych, wszystkie Wytyczne powinny być stosowane, a proporcjonalność będzie polegać jedynie na sposobie wdrożenia poszczególnych Wytycznych, uwzględniającym specyfikę prowadzonej działalności oraz wynikające z przyjętej strategii metody realizacji wsparcia przez obszar IT działalności towarzystwa.

4. ORGANIZACJA DOKUMENTU

4.1.1. Model został podzielony na rozdziały poświęcone regulacjom mającym wpływ na sposób implementacji Usług chmury obliczeniowej przez Podmioty nadzorowane w sektorze funduszy inwestycyjnych.

4.1.2. W Rozdziale V. zacytowano zapisy poszczególnych sekcji Komunikatu chmurowego, wskazano jakie są wymagania w stosunku do Podmiotu nadzorowanego i Dostawcy usług chmurowych w danym punkcie, jakie opracowania lub produkty powinny powstać po każdej z zaangażowanych stron, a dodatkowo, tam gdzie było to możliwe w formie odesłania, zaprezentowano przykładowy dokument/szablon, który może być wykorzystany przez Podmiot nadzorowany podczas przygotowania do wdrożenia usługi chmurowej.

4.1.3. W Rozdziale VI. zacytowane zostały przepisy prawne dotyczące tzw. outsourcingu regulowanego wraz z odpowiednim komentarzem dostosowanym do sytuacji, gdy usługa chmury obliczeniowej stanowi jednocześnie taki outsourcing regulowany.

4.1.4. Każdy z podrozdziałów zawiera (o ile ma zastosowanie):

1) zacytowanie w nagłówku rozdziału danego punktu regulacji,
2) podsumowanie opisu wymagań wynikających z danego punktu regulacji,
3) wskazanie zadań - wymagań do zaadresowania (produktów do opracowania) po stronie Podmiotu nadzorowanego, wynikających z zapisów wskazanych wymagań,
4) wskazanie zadań - wymagań do zaadresowania (produktów do opracowania) po stronie Dostawcy, wynikających z zapisów wskazanych wymagań oraz
5) wskazanie szablonów/przykładów dokumentów/zestawień, które adresują niektóre z wymagań regulacji.

4.1.5. Podrozdziały „ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO” oraz „ZADANIA / PRODUKTY PO STRONIE DOSTAWCY” mają na celu wylistowanie wymogów i produktów, jakie wymagają zaadresowania i odniesienia się po każdej ze stron, we właściwym zakresie tematycznym. Pełna lista produktów do opracowania po stronie Podmiotu nadzorowanego, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Podmiotu nadzorowanego” do niniejszego Modelu.

5. KOMUNIKAT – OBJAŚNIENIE WYMOGÓW

5.1. WYTYCZNE STOSOWANIA KOMUNIKATU

IV. WYTYCZNE STOSOWANIA

1. W celu zapewnienia prawidłowego funkcjonowania rynku finansowego, jego stabilności oraz bezpieczeństwa, na podstawie art. 4 ust. 1 ustawy o nadzorze nad rynkiem finansowym, Nadzór oczekuje od podmiotów nadzorowanych stosowania niniejszego modelu referencyjnego podczas działań związanych z przygotowaniem, realizacją oraz zakończeniem przetwarzania informacji w chmurze obliczeniowej, traktując go jako sprecyzowanie istniejących wymagań prawnych oraz bez uszczerbku dla tych wymagań, jeżeli:
   1) przetwarzane informacje należą do informacji prawnie chronionych w rozumieniu niniejszego komunikatu lub
   2) przetwarzanie informacji ma charakter outsourcingu szczególnego chmury obliczeniowej w rozumieniu niniejszego komunikatu i przetwarzanie informacji jest realizowane w chmurze obliczeniowej publicznej lub hybrydowej (w zakresie jej części opartej o chmurę obliczeniową publiczną).
2. Nadrzędnym zadaniem podmiotu nadzorowanego podczas przetwarzania informacji w chmurze obliczeniowej jest zapewnienie bezpieczeństwa przetwarzanych informacji oraz zgodności sposobu i zakresu tego przetwarzania z prawem. Stosowanie tego komunikatu powinno odbywać się z poszanowaniem zasady proporcjonalności przy równoległym uwzględnieniu modelu referencyjnego. Zasada proporcjonalności powinna znaleźć swoją konkretyzację na etapie szacowania ryzyka związanego z planowaniem czynności przetwarzania oraz adekwatnością stosowanych zabezpieczeń przetwarzanych informacji. UKNF podkreśla, że zasada proporcjonalności nie powinna być interpretowana jako przyzwolenie na zastosowanie przez mniejsze podmioty nadzorowane mniej efektywnych zabezpieczeń przetwarzanych informacji niż opisane w niniejszym komunikacie.
3. Nadzór podkreśla, że opisane w niniejszym komunikacje wymagania powinny być stosowane przez podmioty nadzorowane przed rozpoczęciem przetwarzania informacji w chmurze obliczeniowej.
4. W celu właściwego stosowania postanowień niniejszego komunikatu podmiot nadzorowany powinien określić dla każdej planowanej do wykorzystania lub wykorzystywanej usługi chmury obliczeniowej:
   1) czy przetwarzane są informacje prawnie chronione oraz
   2) czy czynność przetwarzania może być definiowana jako outsourcing szczególny chmury obliczeniowej.

MATRYCA STOSOWANIA KOMUNIKATU		OUTSOURCING CHMURY OBLICZENIOWEJ	
		Inny niż szczególny	Szczególny
INFORMACJE	Inne niż prawnie chronione	Komunikat może być stosowany.	Komunikat powinien być stosowany.
	Prawnie chronione	Komunikat powinien być stosowany.	

5. W przypadku kwalifikowania czynności lub informacji do więcej niż jednej kategorii według powyższej matrycy, należy przyjąć do stosowania wymaganie bardziej rygorystyczne.
6. Niezależnie od powyższego, komunikatu nie stosuje się, gdy stosowny, szczególny przepis prawa:
   1) wyklucza możliwość przetwarzania w chmurze obliczeniowej określonej informacji lub wyklucza możliwość wykonywania w chmurze obliczeniowej określonych czynności przetwarzania;
   2) nakłada wymóg spełnienia określonych wymagań technicznych lub organizacyjnych dotyczących przetwarzania określonych informacji, które wykluczałyby możliwość spełnienia wymagań niniejszego komunikatu.
7. Niniejszy komunikat nie musi być stosowany podczas projektowania i eksploatacji środowisk testowych lub rozwojowych w chmurze obliczeniowej, o ile w środowiskach tych nie są przetwarzane informacje prawnie chronione.
8. Komunikat nie dotyczy przetwarzania informacji w chmurze obliczeniowej prywatnej.

OPIS WYMAGAŃ

5.1.1. Komunikat jest wiążący wyłącznie w stosunku do Podmiotu nadzorowanego. Dostawca i poddostawcy nie są związani wymogami Komunikatu chmurowego.

5.1.2. Komunikat musi być stosowany w dwóch przypadkach:

1) przetwarzania Tajemnicy zawodowej w ramach Outsourcingu chmury obliczeniowej lub

2) Outsourcingu szczególnego chmury obliczeniowej.

5.1.3. W każdym innym przypadku Komunikat może być stosowany, jeśli Podmiot nadzorowany (również w porozumieniu z Dostawcą) tak postanowi.

5.1.4. Komunikat nie stosuje się do Chmury obliczeniowej prywatnej, w tym Chmury obliczeniowej społecznościowej o charakterze prywatnym.

5.1.5. Podmiot nadzorowany określa typ przetwarzanych danych (informacji) dla danej Usługi chmury obliczeniowej, ze względu na Tajemnicę zawodową oraz typ czynności ze względu na Outsourcing szczególny chmury obliczeniowej.

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.1.6. Dokument potwierdzający przeprowadzenie analizy w zakresie typu przetwarzanych danych (informacji), planowanej Usługi chmury obliczeniowej oraz rodzaju czynności przetwarzania i jej kwalifikacji (może być to część dokumentu klasyfikacji i oceny informacji).

5.1.7. Dokument potwierdzający przeprowadzenie analizy w odniesieniu do wymagań Outsourcingu szczególnego chmury obliczeniowej.

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.1.8. Brak

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

5.1.9. Brak

5.2. WYTYCZNE DO KLASYFIKACJI I OCENY INFORMACJI

V. WYTYCZNE DO KLASYFIKACJI I OCENY INFORMACJI

1. Podmiot nadzorowany przeprowadza w udokumentowanym procesie klasyfikację:
   1) informacji prawnie chronionych w rozumieniu niniejszego komunikatu;
   2) informacji, których ochrona wynika z uregulowań prawnych nieuwzględnionych w niniejszym komunikacie;
   3) informacji, które nie podlegają ochronie prawnej.
2. Ocena informacji przeprowadzona jest pod kątem dopuszczalności ich przetwarzania w chmurze obliczeniowej, w szczególności biorąc pod uwagę:
   1) zgodność z wymaganiami prawa oraz specyficznymi dla danego sektora lub podmiotu nadzorowanego postanowieniami oraz zobowiązaniami umownymi;
   2) zakres klasyfikowanych informacji, ich rodzaj i ważność;
   3) wartość informacji dla podmiotu nadzorowanego.
3. Podmiot nadzorowany w procesie klasyfikacji i oceny informacji uwzględnia:
   1) skalę prowadzonej działalności;
   2) korporacyjne, grupowe lub inne modele lub metody oceny i klasyfikacji, które uwzględniają powyższe założenia i są wspólne dla grupy podmiotów, do których zalicza się podmiot nadzorowany;
   3) odpowiedzialność podmiotu nadzorowanego za przetwarzane informacje.
4. Podmiot nadzorowany powinien przeprowadzić klasyfikację i ocenę informacji ponownie, gdy:
   1) zamierza przetwarzać nowy rodzaj informacji;
   2) zamierza wykorzystać nową usługę chmury obliczeniowej;
   3) zmiana prawa, regulacji, regulaminów lub postanowień umów, których stroną jest podmiot nadzorowany, wpływa albo może wpływać na zgodność postępowania podmiotu nadzorowanego w kontekście przetwarzania informacji w chmurze obliczeniowej;
   4) istotnie zwiększa się albo zmniejsza skala przetwarzania;
   5) istotnie zwiększa się wartość przetwarzanych informacji.

5. Podmiot nadzorowany powinien regularnie (nie rzadziej niż raz w roku) przeglądać i potwierdzać aktualność stosowanej klasyfikacji i oceny informacji do bieżących warunków swojego działania.

OPIS WYMAGAŃ

5.2.1. Podmiot nadzorowany powinien opracować lub zaktualizować swoje procedury w zakresie klasyfikacji i oceny informacji, uwzględniając wymogi Komunikatu.

5.2.2. Podmiot nadzorowany powinien przeprowadzić klasyfikację i ocenę informacji dla danej usługi chmury obliczeniowej, zgodnie z przyjętymi w Podmiocie nadzorowanym procedurami.

5.2.3. Podmiot nadzorowany powinien na bieżąco monitorować zmiany wymogów prawnych oraz regulacyjnych w zakresie, który wymagałby ponownej klasyfikacji przetwarzanych informacji. Ponowna klasyfikacja przetwarzanych danych może być także wymagana w sytuacji, gdy rozszerzeniu ulega zakres dotychczasowej usługi chmurowej.

5.2.4. Podmiot nadzorowany powinien, nie rzadziej niż raz w roku, przeglądać i potwierdzać aktualność stosowanej klasyfikacji i oceny informacji w odniesieniu do bieżących warunków swojej działalności.

5.2.5. Właściwie przeprowadzony proces klasyfikacji informacji przetwarzanej w chmurze obliczeniowej pozwoli Podmiotowi nadzorowanemu właściwie wykonać analizę ryzyka, a w konsekwencji dobrać adekwatne mechanizmy oraz zidentyfikować narzędzia i procesy zapewniające należyty poziom bezpieczeństwa. Biorąc pod uwagę istotność procesu klasyfikacji informacji, Podmiot nadzorowany może wykorzystać listę pytań kontrolnych z Załącznika nr 3 „Klasyfikacja informacji" podczas oceny dojrzałości istniejących w Podmiocie nadzorowanym procesów, a ewentualne braki uzupełnić, wprowadzając stosowne zmiany do procesów i polityk.

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.2.6. Udokumentowany proces klasyfikacji i oceny informacji przetwarzanych w chmurze obliczeniowej dla danej usługi chmury obliczeniowej.

5.2.7. Udokumentowane wyniki klasyfikacji danych (informacji), które powinny zostać uwzględnione w planie przetwarzania danych (informacji) w chmurze obliczeniowej dla danej usługi chmury obliczeniowej.

5.2.8. Udokumentowany standard klasyfikacji danych (informacji) stosowany przez Podmiot nadzorowany.

5.2.9. Poinformowanie Podmiotu nadzorowanego o planie zmiany miejsca przetwarzania danych (informacji) w chmurze obliczeniowej, jeśli taka zmiana ma nastąpić w stosunku do uzgodnień umowy zawartej między stronami.

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

5.2.10. **Załącznik nr 2** – Klasyfikacja informacji - skoroszyt.

5.2.11. **Załącznik nr 3** – Klasyfikacja informacji – opis zagadnień.

5.3. WYTYCZNE DO SZACOWANIA RYZYKA

VI. WYTYCZNE DO SZACOWANIA RYZYKA

1. Podmiot nadzorowany prowadzi w udokumentowanym procesie kompleksowe szacowanie ryzyka (identyfikację, analizę oraz ocenę zagrożeń, możliwość ich wystąpienia oraz wpływ tego wystąpienia na podmiot nadzorowany), zgodnie z wymaganiami aktualnego wydania normy PN-ISO 27005 (Zarządzanie ryzykiem w bezpieczeństwie informacji) lub jej odpowiednika w europejskim systemie normalizacji, lub na bazie innego, usystematyzowanego podejścia. Szacowanie ryzyka jest prowadzone w sposób ciągły, z uwzględnieniem praktycznej implementacji zasady PDCA („plan – do – check – act").
2. Podmiot nadzorowany uwzględnia w procesie szacowania ryzyka, w kontekście wyników przeprowadzonej klasyfikacji i oceny przetwarzanych informacji w chmurze obliczeniowej, co najmniej:
   1) Ogólne zagrożenia dla stosowania chmury obliczeniowej:
      a) rozproszenie geograficzne przetwarzanych informacji, w szczególności w kontekście zapewnienia zgodności procesu przetwarzania informacji z przepisami prawa, regulacjami wewnętrznymi, zobowiązaniami umownymi oraz deklaracjami i innymi uregulowaniami;
      b) możliwość utraty zgodności postępowania podmiotu nadzorowanego z przepisami prawa (w tym wydanych licencji lub zezwoleń) poprzez korzystanie z usług chmury obliczeniowej w sposób niezamierzony albo inny niż zamierzony;
      c) dostęp do przetwarzanych informacji przez pracowników i współpracowników (np. poddostawców) dostawcy usług chmury obliczeniowej;
      d) dostęp do przetwarzanych informacji, gwarantowany przez jurysdykcję kraju, w którym odbywa się fizycznie przetwarzanie (lokalizacja centrum przetwarzania danych), w szczególności odniesienie do katalogu sytuacji (lub podmiotów), w której możliwe jest żądanie informacji lub dostępu do nich bez wyraźnej zgody podmiotu nadzorowanego, zarówno przez organy administracji krajowej jak i międzynarodowej;
      e) brak zgodności technologicznej pomiędzy usługami różnych dostawców chmury obliczeniowej powodujące przywiązanie do jednego dostawcy usług chmury obliczeniowej poprzez ograniczenie albo brak możliwości przenoszenia (korzystania z identycznych) usług lub przetwarzanych informacji (vendor lock-in);
      f) awarie mechanizmów izolacji zasobów używanych do świadczenia usług chmury obliczeniowej;
      g) podatność interfejsów zarządzających usługami, które są udostępniane przez dostawców usług chmury obliczeniowej;
      h) ograniczona możliwość wpływania na zakres, kształt i zmiany usług, w tym w szczególności na proces retencji przetwarzanych informacji oraz ich usuwania po zakończeniu realizacji usług przetwarzania;
      i) ograniczona możliwość kontrolowania dostawcy usług chmury obliczeniowej oraz jego poddostawców, w tym bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usług chmury obliczeniowej;

j) podział odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy dostawcę usług chmury obliczeniowej a podmiot nadzorowany;

1) Specyficzne zagrożenia dla stosowanych konkretnych (nazwanych) usług chmury obliczeniowej:
   a) możliwości korzystania z usług w sposób niezgodny z intencjami podmiotu nadzorowanego lub w środowisku, które nie podlega kontroli podmiotu nadzorowanego (np. prywatne urządzenia mobilne, dostęp z prywatnych lub publicznych sieci);
   b) możliwości jednostronnej zmiany warunków technicznych korzystania z usługi (w szczególności jej parametrów lub zasad konfiguracji);
   c) stosowanie domyślnych lub publicznie dostępnych parametrów konfiguracyjnych usług, bez ich należytej weryfikacji i oceny adekwatności dla potrzeb podmiotu nadzorowanego;
   d) stosowane mechanizmy uwierzytelniania oraz ich słabości;
2) Specyficzne zagrożenia związane z zasobami podmiotu nadzorowanego:
   a) wymagane i posiadane zasoby, w tym zasoby ludzkie o ustalonych kompetencjach;
   b) zgodność technologiczna posiadanego środowiska teleinformatycznego oraz środowiska chmury obliczeniowej, a w szczególności mechanizmy integracji;
3) Wartość przetwarzanych informacji dla podmiotu nadzorowanego oraz skutki bezpośrednie i pośrednie utraty kontroli nad ich przetwarzaniem;
4) Stanowisko nadzoru w sprawie szyfrowania informacji, zgodnie z którym:
   a) szyfrowanie informacji nie zmniejsza ważności informacji, nie zmienia też jej klasyfikacji i oceny;
   b) szyfrowanie informacji oraz właściwe zarządzanie kluczami szyfrującymi zapobiega ujawnieniu informacji;
   c) brak jest gwarancji dla uznania danego algorytmu szyfrowania za „całkowicie bezpieczny". Nadzór zaleca używanie algorytmów szyfrowania, które – bazując na dostępnych publicznie informacjach
   (np. opracowaniach merytorycznych, raportach jednostek zajmujących się cyberbezpieczeństwem lub kryptografią) – nie są uznane za skompromitowane. W przypadku używania algorytmu uznanego za skompromitowany, podmiot nadzorowany powinien niezwłocznie podjąć działania w celu zapewnienia bezpieczeństwa przetwarzanych informacji;
   d) informacje przetwarzane w chmurze obliczeniowej powinny być szyfrowane zawsze, gdy to jest technologicznie możliwe i – w ocenie podmiotu nadzorowanego – ekonomicznie zasadne;

e) informacje prawnie chronione muszą być szyfrowane zawsze „at rest” oraz „in transit”. Nadzór dopuszcza sytuację, w której informacje prawnie chronione są szyfrowane „at rest” natychmiast po ich przesłaniu do chmury obliczeniowej przy założeniu jednoczesnego stosowania szyfrowania „in transit” i nie traktuje takiej sytuacji jako ujawnienia przetwarzanych informacji;

f) 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;

5) 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;

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;

6) Stanowisko nadzoru w sprawie usług (dostawców usług chmury obliczeniowej), które są wykorzystywane do świadczenia własnych usług przez bezpośrednich dostawców podmiotów nadzorowanych, zgodnie z którym:

a) podmiot nadzorowany powinien upewnić się, w jakim zakresie świadczona przez bezpośredniego dostawcę usługa wykorzystuje usługi chmury obliczeniowej, a w szczególności czy dochodzi do przetwarzania informacji prawnie chronionej w usłudze chmury obliczeniowej;

b) zależnie od faktycznego wykorzystania usług chmury obliczeniowej oraz zakresu przetwarzanych informacji podmiot nadzorowany powinien zapewnić, że przetwarzanie informacji jest realizowane z uwzględnieniem postanowień niniejszego komunikatu;

7) Stanowisko nadzoru w sprawie prawa właściwego umowy pomiędzy dostawcą usług chmury obliczeniowej a podmiotem nadzorowanym, zgodnie z którym:

a) prawem właściwym dla umowy jest prawo polskie lub prawo innego państwa członkowskiego Unii Europejskiej, chyba że strony umowy poddadzą umowę prawu państwa trzeciego, a prawo państwa trzeciego pozwala na skuteczne wykonywanie:

i. postanowień umowy;

ii. wszystkich wymogów prawa polskiego ciążących na podmiocie nadzorowanym;

iii. wytycznych organu nadzoru, w tym również w zakresie niniejszego komunikatu;

b) w przypadku poddania umowy prawu państwa trzeciego podmiot nadzorowany powinien posiadać pisemną opinię prawną potwierdzającą, że zgodnie z wybranym prawem właściwym umowy wszystkie postanowienia umowy pomiędzy podmiotem nadzorowanym a dostawcą usług chmury obliczeniowej spełniają wymagania prawa obowiązujące podmiot nadzorowany oraz wymagania niniejszego komunikatu;

8) Inne istotne zagrożenia, które podmiot nadzorowany identyfikuje w związku z wykorzystywaniem usług chmury obliczeniowej.

3. Podmiot nadzorowany w procesie szacowania ryzyka powinien uwzględnić możliwość:

1) korzystania ze zweryfikowanych, aktualizowanych źródeł informacji o zagrożeniach specyficznych dla stosowania usług chmury obliczeniowej, w tym również w odniesieniu do konkretnych (nazwanych) usług;

2) korzystania z pomocy ze strony podmiotów lub osób o specjalistycznych kompetencjach zarówno w obszarze cyberbezpieczeństwa jak i usług chmury obliczeniowej, szczególnie w sytuacji braku takich kompetencji wewnątrz własnej organizacji podmiotu nadzorowanego;

3) przeanalizowania dostępnych wyników audytów zewnętrznych dostawców usług chmury obliczeniowej w odniesieniu do usług chmury obliczeniowej oraz procesu zarządzania bezpieczeństwem informacji, poszerzając zakres analizy o dostępne certyfikaty wystawione dostawcy usług chmury obliczeniowej potwierdzające spełnienie wymagań;

4) uprzedniego testowania usług chmury obliczeniowej, także przy wykorzystaniu scenariuszy warunków skrajnych, zarówno w zakresie sposobu działania usługi jak i jej konfiguracji.

4. Podmiot nadzorowany, na podstawie wyników szacowania ryzyka, zarządza tym ryzykiem, uwzględniając w szczególności:

1) wymagania przepisów prawa, regulacji wewnętrznych oraz postanowień umownych;

2) stopień złożoności organizacyjnej, podział uprawnień i odpowiedzialności podmiotu nadzorowanego, zawarte porozumienia, oraz analogiczne czynniki występujące w grupie kapitałowej lub organizacji grupowej, lub o charakterze stowarzyszenia, do których podmiot nadzorowany należy;

3) Efektywność stosowanych mechanizmów kontrolnych i monitorujących, zwłaszcza w odniesieniu do:

   a) identyfikacji nowych zagrożeń;

   b) zmian w wykorzystywanej usłudze chmury obliczeniowej lub trybie i zakresie jej wykorzystywania;

   c) zmian w relacji z dostawcą usług chmury obliczeniowej, w tym możliwość również nieplanowanego zakończenia współpracy zarówno przez podmiot nadzorowany jak i dostawcę usług chmury obliczeniowej;

4) Kompetencje techniczne i zdolności organizacyjne podmiotu nadzorowanego, w szczególności w kontekście bezpiecznego wykorzystywania usług chmury obliczeniowej oraz realizacji postanowień umownych;

5) Zdolność podmiotu nadzorowanego i zgodność z przepisami prawa do transferowania zidentyfikowanego ryzyka lub akceptacji oszacowanego poziomu ryzyka.

5. Wyniki szacowania ryzyka powinny dawać podstawę do twierdzenia, że świadczenie usługi chmury obliczeniowej będzie realizowane zgodnie z wymaganiami prawa obowiązującymi podmiot nadzorowany, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi przez podmiot nadzorowany standardami.

6. Wyniki szacowania ryzyka powinny zostać formalnie zatwierdzone oraz podlegać okresowej weryfikacji i aktualizacji. Zatwierdzenie powinno obejmować decyzję podmiotu nadzorowanego dotyczącą:

   1) Usług chmury obliczeniowej, z których podmiot nadzorowany będzie korzystał;

   2) Rodzaju i zakresu przetwarzanych w ramach tych usług informacji.

OPIS WYMAGAŃ

5.3.1. Podmiot nadzorowany powinien opracować lub zaktualizować swoje procedury w zakresie szacowania i oceny ryzyka, w zakresie korzystania z Usług chmury obliczeniowej, uwzględniając przy tym wymogi Komunikatu.

5.3.2. Zgodnie z postanowieniami Komunikatu, dla danej Usługi chmury obliczeniowej, Podmiot nadzorowany powinien przeprowadzić kompleksowe szacowanie ryzyka, biorąc pod uwagę wszelkie zidentyfikowane zagrożenia, ocenę prawdopodobieństwa ich wystąpienia oraz ewentualnego wpływu na Podmiot nadzorowany.

5.3.3. Podmiot nadzorowany powinien nie rzadziej niż raz w roku zweryfikować czynniki mające istotny wpływ na szacowanie ryzyka (w tym wymogi prawne, regulacyjne, organizacyjne oraz techniczne) i w przypadku zaistnienia takich czynników dokonać ponownego szacowania ryzyka.

5.3.4. Komunikat wskazuje 21 zagrożeń w dwóch kategoriach: ogólne zagrożenia do stosowania chmury obliczeniowej oraz specyficzne zagrożenia do stosowanych konkretnych usług chmury obliczeniowej. Jest to minimalna lista zagrożeń, jaką należy przeanalizować. Można ją powiększać o dodatkowe zidentyfikowane zagrożenia, mające potencjalny wpływ na korzystanie z Usługi chmury obliczeniowej. W odpowiedzi na zapis w pkt 2. ppkt 9) Komunikatu, prezentujemy listę przykładowych zagrożeń i podatności, która została zawarta w Załączniku nr 5 „Lista przykładowych zagrożeń i podatności" do niniejszego opracowania.

5.3.5. Jako Załącznik nr 4 załączony jest Szablon szacowania ryzyka, jaki można wykorzystywać w celu przeprowadzenia szacowania ryzyka przetwarzania informacji w chmurze.

5.3.6. Poniżej znajdują się komentarze do wybranych ryzyk wskazanych w Komunikacie:

1) Pkt 2 ppkt 4) – *Podmiot nadzorowany uwzględnia w procesie szacowania ryzyka […] wartość przetwarzanych informacji dla podmiotu nadzorowanego oraz skutki bezpośrednie i pośrednie utraty kontroli nad ich przetwarzaniem."* Określenie „wartości" przetwarzanych informacji nie powinno być interpretowane jako wymóg oszacowania wartości pieniężnej danej informacji, gdyż w praktyce dokonywanie takiej ewaluacji wydaje się być zbyt czasochłonne i kosztowne dla danego procesu wdrożenia Usługi chmury obliczeniowej. Pojęcie „wartość" semantycznie powinno korespondować z pojęciem „ważność" również używanym w Komunikacie.

2) Pkt 2 ppkt 6) – „*Stanowisko nadzoru w sprawie tworzenia łańcucha outsourcingowego*". Objaśnienia w zakresie podoutsourcingu znajdują się w pkt. 6. Modelu.

3) UKNF w Q&A chmurowym wskazuje, że „w sytuacji, gdy podmiot nadzorowany, dokonując analizy ryzyka i jego oszacowania stwierdzi, że poprzez relację umowną z dostawcą oprogramowania nie jest w stanie zagwarantować realizacji postanowień Komunikatu przez poddostawcę, Podmiot nadzorowany powinien:

   a) nawiązać relację umowną z poddostawcą (dostawcą chmurowym) w celu realizacji postanowień Komunikatu (np. w formule umowy trójstronnej);

   b) zrezygnować z usług świadczonych przez dostawcę oprogramowania, jeżeli niezależnie od formy relacji (np. umowa z poddostawcą) nie będzie możliwe zagwarantowanie wykonania postanowień Komunikatu".

4) UKNF krytycznie ocenia wyłączenia albo ograniczenia odpowiedzialności dostawcy usług chmury obliczeniowej oraz jego poddostawców wobec podmiotu nadzorowanego, nawet jeśli znajdują się one w granicach szczególnych przepisów prawa, w następujących sytuacjach:

   a) 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

   b) przetwarzanie ma charakter outsourcingu szczególnego chmury obliczeniowej.

5) Biorąc pod uwagę powyższe oczekiwanie UKNF, decyzja o ewentualnej akceptacji ograniczeń lub wyłączeń odpowiedzialności (o ile dopuszczalna powszechnie obowiązującymi przepisami prawa) powinna być podjęta na podstawie rzetelnej oceny ryzyka wynikającego z takiego ograniczenia dla danej Usługi chmury obliczeniowej. Przy podejmowaniu ww. decyzji należy wziąć pod uwagę dopuszczalność akceptacji ograniczenia z punktu widzenia zarządzania Podmiotem nadzorowanym oraz to, czy takie ograniczenie odpowiedzialności jest dla Podmiotu nadzorowanego ekonomicznie akceptowalne.

6) Komunikat wymaga, aby szacowanie ryzyka dla danej Usługi chmury obliczeniowej było przeprowadzone i udokumentowane w sposób zgodny z przyjętą przez Podmiot nadzorowany metodyką, zakładającą, oczekiwany przez nadzór, proces ciągłego monitorowania ryzyka, związanego m.in. z wykorzystywaniem usług chmury obliczeniowej. Komunikat jako przykład udokumentowanego procesu podaje aktualne wydanie normy PN-ISO 27005 (Zarządzanie ryzykiem w bezpieczeństwie informacji) lub jej odpowiednika w europejskim systemie normalizacji. Zastosowanie ww. norm ISO nie jest konieczne, dopuszczalne jest wykorzystanie innego, właściwego dla Podmiotu nadzorowanego, usystematyzowanego podejścia.

7) Wymagania określone w pkt 5. i 6. wyżej cytowanego fragmentu Komunikatu chmurowego mogą być rozumiane następująco:

   a) Sposób zatwierdzania wyników szacowania ryzyka dla Usługi chmury obliczeniowej może być wskazany w odpowiedniej polityce zarządzania ryzykiem, polityce bezpieczeństwa teleinformatycznego lub innym równoważnym dokumencie.

   b) Wyniki szacowania ryzyka dla danej Usługi chmury obliczeniowej powinny potwierdzać, że usługa będzie realizowana zgodnie z obowiązującymi przepisami prawa, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi przez Podmiot nadzorowany standardami działania. W związku z tym, dokument zawierający takie „wyniki szacowania ryzyka" obejmować powinien następujące oświadczenie „Świadczenie usługi chmury obliczeniowej będzie realizowane zgodnie z wymaganiami prawa obowiązującymi Podmiot nadzorowany, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi standardami."

   c) Formalne zatwierdzenie „wyników szacowania ryzyka" następuje w sposób właściwy dla akceptacji procesów ze względu na ich istotność lub znaczenie opisanych w odpowiednich dokumentach wewnętrznych danej organizacji. Dla procesów krytycznych lub istotnych przetwarzanych w Usłudze chmury obliczeniowej może okazać się konieczna uchwała zarządu Podmiotu nadzorowanego.

   d) Weryfikacja i aktualizacja następują według zasad właściwych dla przeglądania i potwierdzania aktualności stosowanej klasyfikacji i oceny informacji (przy czym obie te czynności przeprowadzić można jednocześnie/łącznie).

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.3.7. Udokumentowana analiza ryzyka dla danej usługi.

5.3.8. Udokumentowana ocena wartości przetwarzanych informacji dla danej usługi.

5.3.9. Udokumentowane dla danej usługi zastosowane metody szyfrowania informacji.

5.3.10. Udokumentowana procedura zarządzania kluczami szyfrującymi.

5.3.11. Udokumentowane potwierdzenie, że zastosowane w danej usłudze algorytmy szyfrowania nie są uznane za skompromitowane.

5.3.12. Udokumentowana ocena, że szyfrowanie w ramach danej usługi jest technologicznie możliwe i ekonomicznie zasadne.

5.3.13. Udokumentowana ocena tworzenia łańcucha outsourcingowego w ramach danej usługi.

5.3.14. Jeśli dotyczy, pisemna opinia prawna w przypadku poddania umowy z dostawcą usługi chmurowej prawu państwa trzeciego.

5.3.15. Udokumentowana lista przeanalizowanych audytów zewnętrznych/certyfikatów wystawionych dostawcy usług chmurowych.

5.3.16. Udokumentowany raport z testów dla danej usługi.

5.3.17. Udokumentowany opis mechanizmów kontrolnych i monitorujących, stosowanych w Podmiocie nadzorowanym.

5.3.18. Opis kompetencji technicznych i zdolności organizacyjnych w kontekście wykorzystywania usług chmurowych oraz realizacji postanowień umownych.

5.3.19. Udokumentowane potwierdzenie zdolności i zgodności z przepisami prawa do transferowania zidentyfikowanego ryzyka lub akceptacji oszacowanego poziomu ryzyka.

5.3.20. Udokumentowane potwierdzenie, że świadczenie danej usługi będzie realizowane zgodnie z wymaganiami prawa, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi standardami.

5.3.21. Udokumentowana decyzja dotycząca korzystania z danej usługi.

5.3.22. Dodatkowo, wychodząc naprzeciw oczekiwaniom nadzoru w zakresie ciągłego monitowania wszystkich aspektów usługi chmurowej, a przede wszystkim: jakości świadczonej usługi, bezpieczeństwa przetwarzanych informacji oraz ryzyka związanego z usługą, w ramach prac nad niniejszą wersją Modelu opracowano propozycję podejścia do monitorowania umowy z Dostawcą usług chmury obliczeniowej. Dokument stanowi Załącznik nr 6 „Kwestionariusz - okresowe monitorowanie umów" do niniejszego opracowania.

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.3.23. W procesie szacowania ryzyka Podmiot nadzorowany powinien uwzględnić informacje pozyskane od Dostawcy usługi chmurowej, w tym udokumentowane spełnienie wymagań lub opis posiadanego stanu, w szczególności w zakresie:

1) Rekomendowane jest uzyskanie raportów z audytów potwierdzających stosowanie metod zabezpieczeń oraz raporty potwierdzające ich skuteczność (odpowiednio np. raporty SOC typu 1. i 2.);

2) Lokalizacji CPD, obszaru przetwarzania danych (lokalizacji Centrum Przetwarzania Danych Dostawcy, z których personel uzyskuje dostęp do danych Podmiotu nadzorowanego); dopuszczalne jest określenie tego na poziomie kraju/regionu (jednostki administracyjnej, rejonu Dostawcy);

3) Sposobu kontroli i monitorowania dostępu do przetwarzanych informacji przez personel Dostawcy i jego poddostawców;

4) Opisu mechanizmów izolacji zasobów używanych do świadczenia Usługi chmury obliczeniowej, wraz z informacją o potencjalnych skutkach awarii mechanizmów izolacji;

5) Dokumentacji interfejsów zarządzających usługą chmury obliczeniowej, informacji o zabezpieczeniach interfejsów i ew. o ich podatnościach;

6) Zasad żądania wprowadzania zmian w zakresie oferowanej usługi przez Dostawcę;

7) Możliwości kontrolowania Dostawcy oraz jego poddostawców, bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usługi chmury obliczeniowej;

8) Podziału odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy Dostawcę i Podmiot nadzorowany;

9) Mechanizmów kontroli dostępu do usługi dla użytkowników, w szczególności metod ograniczenia dostępu z urządzeń prywatnych;

10) Możliwości integracji z innymi, wskazanymi przez Podmiot nadzorowany technologiami;

11) Stosu technologicznego w obszarze zapewnienia bezpieczeństwa środowiska, danych (informacji) oraz zasobów chmury obliczeniowej, w szczególności mechanizmów szyfrowania;

12) Łańcucha outsourcingowego oraz procesu kontroli i zapewnienia jakości usługi.

5.3.24. Przykładowy zestaw wymagań w stosunku do Dostawcy usług chmurowych znajduje się w dwóch Załącznikach do niniejszego Modelu – ‘Ankiecie wymagań dla dostawców usługi chmurowej’ (Załącznik nr 8) oraz ‘Ankiecie dla dostawców – udokumentowanie konfiguracji usługi’ (Załącznik nr 9).

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.3.25. **Załącznik 1** – Lista produktów do opracowania po stronie Podmiotu nadzorowanego.

5.3.26. **Załącznik 4** – Szablon szacowania ryzyka.

5.3.27. **Załącznik 5** – Lista przykładowych zagrożeń i podatności.

5.3.28. **Załącznik 6** – Kwestionariusz - okresowe monitorowanie umów.

5.3.29. **Załącznik 8** – Ankieta dla dostawców usługi chmurowej.

5.3.30. **Załącznik 9** – Ankieta dla dostawców – udokumentowanie konfiguracji usługi.

5.4. MINIMALNE WYMAGANIA DLA PRZETWARZANIA INFORMACJI W CHMURZE OBLICZENIOWEJ

VII. MINIMALNE WYMAGANIA DLA PRZETWARZANIA INFORMACJI W CHMURZE OBLICZENIOWEJ

1. Niniejsze minimalne wymagania techniczne i organizacyjne dla przetwarzania informacji w chmurze obliczeniowej stanowią referencyjne odniesienie, które podmiot nadzorowany powinien weryfikować pod kątem adekwatności do wyników oszacowania ryzyka oraz zapewnić ich spełnienie.
2. Środki techniczne i zasoby organizacyjne służące bezpieczeństwu przetwarzanych informacji powinny wynikać z przeprowadzonego procesu szacowania ryzyka, jednak – niezależnie od wyników tego szacowania – nie mogą osłabiać wymagań opisanych poniżej.
3. Zapewnienie kompetencji:
   1) Podmiot nadzorowany zapewnia w udokumentowanym procesie właściwe kompetencje dla planowanych lub prowadzonych działań przetwarzania informacji w środowisku chmury obliczeniowej. Kompetencje te zawierają wymagania w odniesieniu do wykształcenia, wyszkolenia, umiejętności i doświadczenia pracowników lub współpracowników podmiotu nadzorowanego zaangażowanych w proces planowania, realizacji, testowania i utrzymywania przetwarzania informacji w chmurze obliczeniowej oraz zawierania i przeglądania umowy z tym związanej.
   2) Podmiot nadzorowany zapewnia rozumienie konsekwencji stosowania określonej architektury chmury obliczeniowej, zasad konfiguracji, podziału odpowiedzialności za bezpieczeństwo przetwarzanych informacji, zależnie od zakresu i rodzaju planowanego lub stosowanego środowiska chmury obliczeniowej oraz modelu świadczonej usługi, z uwzględnieniem wymagań ciągłości działania podmiotu nadzorowanego oraz posiadanej infrastruktury teleinformatycznej. Rozumienie konsekwencji danego wyboru ma odniesienie w dokumentacji szacowania ryzyka, zapewnieniu właściwych zasobów zarówno pod względem jakościowym jak i ilościowym oraz dodatkowo we wszystkich pracach (oraz umowach) związanych z tworzeniem lub rozwojem oprogramowania przeznaczonego do używania w chmurze obliczeniowej oraz integracji usług bazujących na zasobach własnych podmiotu nadzorowanego.
   3) Kompetencje pracowników lub współpracowników podmiotu nadzorowanego odpowiedzialnych za bezpieczeństwo oraz planowanie, konfigurację i zarządzanie oraz monitoring usług chmury obliczeniowej powinny być potwierdzone odpowiednią dokumentacją szkoleniową lub imiennymi zaświadczeniami w zakresie odpowiednim do używanych usług chmury obliczeniowej (lub wynikać z umiejętności i doświadczenia), w tym również specyficznych lub specyficznie konfigurowanych dla danego dostawcy usług chmury obliczeniowej. Wymaganie to odnosi się również do kompetencji osób odpowiedzialnych za przegląd lub weryfikację dokumentacji audytów, certyfikatów i innych dokumentów dostawcy usług chmury obliczeniowej, w tym umowy na świadczenie usług chmury obliczeniowej oraz dokumentów o charakterze technicznym.

OPIS WYMAGAŃ

5.4.1. Podmiot nadzorowany w celu zapewnienia bezpieczeństwa przetwarzanych w Chmurze obliczeniowej informacji, powinien zapewnić właściwy poziom wiedzy i umiejętności personelu (pracowników i współpracowników), przy czym taki właściwy poziom wiedzy i umiejętności określa się co do zasady na podstawie wyników oszacowania ryzyka. Utrzymanie i systematyczne podnoszenie kwalifikacji (wiedzy i umiejętności) powinno być częścią dobrych praktyk Podmiotu nadzorowanego. W przypadku stwierdzenia

ewentualnych braków można je zaadresować poprzez stosowne szkolenia lub skorzystać ze wsparcia firm świadczących usługi konsultacyjno-doradcze w zakresie usług chmury obliczeniowej. W zakresie, w jakim Podmiot nadzorowany realizuje procesy dotyczące obsługi usług chmury obliczeniowej własnymi zasobami, kompetencje pracowników i współpracowników powinny być udokumentowane, np. w formie certyfikatów szkoleniowych lub też certyfikatów Dostawców.

5.4.2. Podmiot nadzorowany powinien określić role w organizacji wraz z zakresem głównych zadań podczas wdrożenia lub przy utrzymaniu rozwiązań chmurowych oraz dopasować do nich wymagane obszary kompetencji. Przykładowymi obszarami ról i dopasowanymi do nich kompetencjami w ramach wdrażania i utrzymania rozwiązań w publicznej Chmurze obliczeniowej są:

1) architektura (rola Architekt);
2) bezpieczeństwo (rola Inżynier bezpieczeństwa);
3) rozwój (role Developer, Inżynier DevOps);
4) utrzymanie (role Administrator, Administrator sieci, Inżynier DevOps);
5) biznes (rola Opiekun biznesowy usługi); oraz
6) finanse (rola Kontroler finansowy).

5.4.3. Role i dopasowane do nich kompetencje powinny zapewniać bezpieczeństwo, spójność architektoniczną oraz dostarczać odpowiednie wsparcie rozwiązań, a także rozliczalność i kontrolę finansową wykorzystywanych Usług chmury obliczeniowej.

5.4.4. Podmiot nadzorowany w ramach utrzymania produkcyjnych systemów przetwarzających informacje w Chmurze obliczeniowej powinien posiadać aktywne wsparcie Dostawców lub korzystać ze wsparcia firm świadczących usługi konsultacyjno-doradcze w zakresie Chmury obliczeniowej.

5.4.5. Właściwy nadzór (ang. governance), pomaga uzyskać pewność, że wdrożone w Chmurze obliczeniowej rozwiązania skutecznie adresują potrzeby biznesowe interesariuszy, zapewniając jednocześnie zgodność regulacyjną. Efektywny nadzór pomaga uzyskać równowagę między realizacją celów i minimalizacją ryzyka. W ocenie skuteczności prowadzonego przez Podmiot nadzorowany nadzoru pomocna może się okazać analiza odpowiedzi na pytania z Załącznika nr 11 ”Nadzór (governance)” dotyczące uwzględnienia w nadzorze aspektów przetwarzania chmurowego.

5.4.6. W Załączniku nr 12 „Wybrane definicje i pojęcia związane z bezpieczeństwem informacji” wyjaśnione zostały pokrótce wybrane definicje i pojęcia związane z bezpieczeństwem informacji.

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.4.7. Udokumentowane potwierdzenie zapewnienia kompetencji projektowych dla projektów chmurowych.

5.4.8. Udokumentowane potwierdzenie zapewnienia kompetencji związanych z zarządzaniem umowami z dostawcami usług chmurowych.

5.4.9. Udokumentowana architektura chmury obliczeniowej dla danej usługi.

5.4.10. Udokumentowane zasady konfiguracji dla danej usługi.

5.4.11. Udokumentowany podział odpowiedzialności między Podmiot nadzorowany i Dostawcę danej usługi chmury obliczeniowej.

5.4.12. Udokumentowane potwierdzenie wykonania szkoleń/posiadania kompetencji w obszarze planowania, konfiguracji, zarządzania oraz monitoringu usług chmury obliczeniowej.

5.4.13. Udokumentowane potwierdzenie wykonania szkoleń/posiadania kompetencji w obszarze bezpieczeństwa usług chmury obliczeniowej.

5.4.14. Udokumentowane potwierdzenie wykonania szkoleń/posiadania kompetencji w obszarze przeglądu lub weryfikacji audytów, certyfikatów i innych dokumentów Dostawcy usług chmury obliczeniowej.

5.4.15. Udokumentowane potwierdzenie wykonania szkoleń/posiadania kompetencji w obszarze przeglądu lub weryfikacji umowy na świadczenie usług chmury obliczeniowej.

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.4.16. Udokumentowane szkolenia, potwierdzone certyfikatami.

5.4.17. Udokumentowane wsparcie personelu Dostawcy na rzecz Podmiotu nadzorowanego.

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.4.18. **Załącznik nr 11** – Nadzór (governance).

5.4.19. **Załącznik nr 12** – Wybrane definicje i pojęcia związane z bezpieczeństwem informacji.

5.5. UMOWA Z DOSTAWCĄ USŁUG CHMURY OBLICZENIOWEJ

4. UMOWA Z DOSTAWCĄ CHMURY OBLICZENIOWEJ.

4.1 Podmiot nadzorowany posiada sformalizowaną umowę (oraz inne dokumenty, w tym oświadczenia, regulaminy, warunki korzystania z usług, także w wersji elektronicznej) z dostawcą usług chmury obliczeniowej, która – tam, gdzie to zasadne w odniesieniu do używanych usług i zakresu przetwarzanych informacji – zawiera lub wskazuje źródła informacji, obejmujące:

a) klarowny podział odpowiedzialności w odniesieniu do bezpieczeństwa przetwarzanych informacji, z uwzględnieniem modelu świadczenia usług, ciągłości działania usług (z uwzględnieniem parametrów RTO i RPO tam, gdzie to zasadne) oraz deklarowanego SLA wraz z metodą pomiaru i raportowania;

b) klarowną definicję i wskazanie lokalizacji przetwarzania informacji oraz metod jej weryfikacji i zabezpieczenia zgodności przez co najmniej referencyjne odniesienie do właściwych dokumentów, opisów konfiguracyjnych, metod i narzędzi;

c) prawo właściwe dla umowy (w tym sąd właściwy i zasady rozstrzygania sporów);

d) potwierdzenie zgodności zasad przetwarzania danych osobowych z prawem Unii Europejskiej, o ile ma to zastosowanie;

e) własność przetwarzanych informacji w trakcie trwania umowy oraz po jej zakończeniu (wygaśnięciu, rozwiązaniu), także w sposób nieplanowany;

f) gwarancje, rękojmie, ubezpieczenia (polisy ubezpieczeniowe dostawcy usług chmury obliczeniowej), kary umowne, określenie siły wyższej, zdarzeń objętych zakresem siły wyższej oraz zasad postępowania w takich sytuacjach, o ile ma to zastosowanie;

g) określenie zakresu odpowiedzialności za szkody wyrządzone klientom podmiotu nadzorowanego (o ile ma to zastosowanie), zgodnie z wymaganiami prawa obowiązującego podmiot nadzorowany;

h) klarowne wskazanie poddostawców (nazwa, lokalizacja, zakres czynności) dostawcy usług chmury obliczeniowej oraz warunki nadawania praw dostępu do informacji przetwarzanych przez podmiot nadzorowany;

i) klarowne wskazanie zasad, zgodnie z którymi zadania, zakresy uprawnień i odpowiedzialności oraz rozliczalność działań poddostawców dostawcy usług chmury obliczeniowej są transparentne i jasno identyfikowane przez podmiot nadzorowany;

j) źródła autoryzowanych informacji o planowanych zmianach w standardach świadczonych usług chmury obliczeniowej (w tym zmianach o charakterze technicznym);

k) źródła dokumentacji technicznej i deklaracji zgodności (w tym zgodności z obowiązującymi przepisami prawa), wraz z instrukcjami dotyczącymi konfiguracji usług chmury obliczeniowej;

l) zakres dodatkowych informacji i dokumentacji przekazywanych przez dostawcę usług chmury obliczeniowej w związku ze świadczeniem usług chmury obliczeniowej;

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);

n) prawo dla nadzoru do wykonania obowiązków kontrolnych, w tym kontroli pomieszczeń i dokumentacji związanej z przetwarzaniem informacji podmiotu nadzorowanego, procesów i procedur, organizacji i zarządzania oraz potwierdzeń zgodności;

o) zasady licencjonowania (w tym prawo do aktualizacji bezpieczeństwa używanego oprogramowania lub jego komponentów) oraz prawa własności intelektualnej, w tym – jeżeli dotyczą – prawo do dysponowania przetwarzanymi informacjami;

p) zasady zmiany treści umowy, w tym parametrów technicznych używanych usług chmury obliczeniowej;

q) zasady rozwiązywania umowy, w tym zasady i terminy zwrotu lub usunięcia przetwarzanych informacji;

r) zasady wsparcia, w tym zakres i okna czasowe (z uwzględnieniem stref czasowych), tryb i sposób zgłaszania problemów z usługami chmury obliczeniowej;

s) zasady wymiany informacji, w tym w szczególności w zakresie bezpieczeństwa oraz zarządzania bieżącymi incydentami, obejmujące zarówno pracowników podmiotu nadzorowanego jak i dostawcy usług chmury obliczeniowej, a w przypadku istotnego narażenia na skutki danego incydentu – również innych stron (np. klientów, poddostawców), w celu zapewnienia adekwatności postępowania do poziomu istotności incydentu.

4.2 Bez uszczerbku dla wymagań prawa oraz z uwzględnieniem postanowień niniejszego komunikatu, podmiot nadzorowany może korzystać z ramowych umów udostępnianych przez dostawców usług chmury obliczeniowej, w szczególności, gdy dotyczą one usług chmury obliczeniowej tworzonych dla grupy podmiotów (w tym podmiotu nadzorowanego) w ramach umów o charakterze korporacyjnym lub grupowym, w tym również chmury obliczeniowej społecznościowej.

W takim przypadku podmiot nadzorowany powinien:

a) zweryfikować w jakim zakresie umowa ramowa oraz powiązane z nią dokumenty, wyniki szacowania ryzyka oraz wymagania prawne, organizacyjne i techniczne uwzględniają postanowienia niniejszego komunikatu oraz są adekwatne dla sytuacji podmiotu nadzorowanego i jego zamiarów związanych z przetwarzaniem informacji w chmurze obliczeniowej;

b) ocenić konieczność lub możliwość samodzielnego stosowania wymagań niniejszego komunikatu w zakresie, który nie jest zgodny z umową ramową i powiązanymi z nią dokumentami.

OPIS WYMAGAŃ

5.5.2. Podmiot nadzorowany jest zobowiązany do zawarcia pisemnej umowy z Dostawcą. Zgodnie z Kodeksem cywilnym, umowa ma formę pisemną gdy jest zawarta na piśmie, przy czym oświadczenie woli złożone w formie elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym jest równoważne formie pisemnej. Formę elektroniczną w rozumieniu Kodeksu cywilnego stanowi wyłącznie kwalifikowany podpis elektroniczny. Rekomendowane jest aby umowy zawierane były co najmniej w wyżej opisanej formie.

5.5.3. Prawem właściwym dla umowy powinno być prawo polskie lub prawo innego państwa członkowskiego Unii Europejskiej. Poddanie umowy prawu państwa trzeciego jest możliwe, o ile prawo takie pozwala na skuteczne wykonywanie:

1) postanowień umowy;

2) wszystkich wymogów prawa polskiego ciążących na Podmiocie nadzorowanym;

3) wytycznych organu nadzoru, w tym również w zakresie Komunikatu.

W przypadku poddania umowy prawu państwa trzeciego, konieczne jest zatem wykonanie analizy prawnej weryfikującej spełnienie powyższych warunków.

5.5.4. Wymogi określone Komunikatem są niezależne od wymogów określonych w przepisach prawa. Te ostatnie, w szczególności opisane w UFI, mogą mieć zastosowanie do umowy Outsourcingu chmury obliczeniowej, o ile ta kwalifikuje się jako umowa Outsourcingu regulowanego. Zagadnienie to omówione jest szerzej w pkt. 6. Modelu.

5.5.5. Umowa z Dostawcą powinna zawierać te elementy (katalog zamknięty) lub wskazywać ich źródła wymienione w pkt. 4.1 fragmentu Komunikatu cytowanego powyżej, które są zasadne w odniesieniu do używanych usług i zakresu przetwarzanych informacji. Dodatkowo, zgodnie z pkt. 4.2 w/w, Podmiot nadzorowany może korzystać z ramowych umów udostępnianych przez Dostawców, przy założeniu braku uszczerbku dla wymagań prawa oraz z uwzględnieniem postanowień Komunikatu. Objaśnienia do wybranych elementów umowy z Dostawcą wskazanych w pkt. 4.1 znajdują się w Załączniku nr 13 „Objaśnienia i lista wybranych klauzul wraz z przykładami".

5.5.6. Podmiot nadzorowany w ramach umowy z Dostawcą powinien mieć jasno określone lokalizacje przetwarzania informacji zarówno u Dostawcy i poddostawców. Umowa nie musi wskazywać dokładnego adresu, jednakże powinna określać co najmniej region geograficzny (np. Warszawa).

5.5.7. Umowa pomiędzy Podmiotem nadzorowanym a jego Dostawcą powinna precyzować warunki oraz zasady dotyczące przeprowadzenia inspekcji w lokalizacjach przetwarzania informacji. Dodatkowo takie same doprecyzowanie powinno dotyczyć wszystkich poddostawców objętych klauzulą audytu 3- strony.

5.5.8. Umowa z Dostawcą powinna zawierać jasno określone zasady usunięcia danych z urządzeń służących do przetwarzania informacji oraz ich backupu.

5.5.9. Umowa z Dostawcą powinna zawierać jasno określone zasady zapewnienia kopii awaryjnych (backup) przetwarzanych informacji, w przypadku, gdy podział odpowiedzialności przewiduje odpowiedzialność dostawcy za zapewnienie kopii awaryjnych przetwarzanych informacji i taka potrzeba wynika z regulacji prawnych.

5.5.10. W odniesieniu do pkt. 4.1 h) Komunikatu cytowanego powyżej, umowa z Dostawcą powinna zawierać ponadto zobowiązanie do informowania Podmiotu nadzorowanego o wszelkich zmianach poddostawców Dostawcy. Podmiot nadzorowany powinien mieć zapewnioną możliwość reagowania na takie zmiany m.in. poprzez wyrażenie sprzeciwu na taką zmianę albo możliwość rozwiązania umowy bez ponoszenia dodatkowych kosztów.

5.5.11. Umowa z Dostawcą usługi chmury obliczeniowej, która kwalifikuje się jako outsourcing regulowany w rozumieniu art. 45a UFI, powinna spełniać również następujące wymogi:

1) Zapewnienie możliwości przekazywania przez Podmiot nadzorowany w każdym czasie dalszych poleceń Dostawcy, jeżeli leży to w interesie uczestników funduszu inwestycyjnego (art. 45a ust. 4 pkt 3) UFI).

2) Zapewnienie prawa do rozwiązania umowy przez Podmiot nadzorowany ze skutkiem natychmiastowym, jeżeli leży to w interesie uczestników funduszu inwestycyjnego (art. 45a ust. 4 pkt 4) UFI).

3) Zapewnienie przez Dostawcę, że posiada niezbędną wiedzę i doświadczenie oraz zapewnia warunki techniczne i organizacyjne niezbędne do prawidłowego wykonania umowy, zapewniające ciągłe i niezakłócone prowadzenie działalności w zakresie objętym umową; (art. 45a ust. 4 pkt 5) UFI)

4) Zapewnienie przez Dostawcę, że znajduje się on w sytuacji finansowej zapewniającej prawidłowe wykonanie umowy (art. 45a ust. 4 pkt 6) UFI);

5) Zasady zapewniające, że Dostawca umożliwi skuteczne nadzorowanie przez Podmiot nadzorowany wykonywania powierzonych mu czynności oraz zarządzanie ryzykiem związanym z powierzeniem czynności (art. 45a ust. 4 pkt 7) UFI).

6) Zapewnienie, że Dostawca umożliwi w każdym czasie skuteczne wykonywanie przez depozytariusza obowiązków wynikających z UFI oraz umowy o wykonywanie funkcji depozytariusza funduszu (art. 45a ust. 4 pkt 8) UFI).

7) W umowie powinny znaleźć się postanowienia zawierające zobowiązania Dostawcy w zakresie ochrony Tajemnicy zawodowej, w tym do przetwarzania tajemnicy zawodowej w zakresie niezbędnym dla realizacji usług.

5.5.12. W ramach prac nad Modelem opracowano propozycję podejścia do monitorowania umowy z Dostawcą usług chmury obliczeniowej. Dokument stanowi Załącznik nr 6 „Kwestionariusz - okresowe monitorowanie umów” do niniejszego opracowania.

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.5.13. Umowa w formie pisemnej z Dostawcą wraz niezbędnymi dokumentami (oświadczenia, regulaminy, warunki korzystania z usług, itp.).

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.5.14. Podpisanie umowy z Podmiotem nadzorowanym, uwzględniającej wymagania Komunikatu i bezwzględnie obowiązujące przepisy prawa.

5.5.15. Dostawca odpowiada za podpisanie umów ze swoimi poddostawcami, które gwarantują możliwość realizacji uprawnień przewidzianych w Umowie. W szczególności, jeśli wymagane jest uprawnienie do przeprowadzenia audytu lub inspekcji w miejscu przetwarzania danych przez Podmiot nadzorowany, Dostawca powinien zapewnić analogiczną możliwość wobec poddostawców.

5.5.16. Dostawca powinien dostarczyć odpowiednie certyfikaty potwierdzające skuteczne usunięcie danych zgodnie z opisem pkt. 4.1.q) fragmentu Komunikatu cytowanego powyżej. Procedura usunięcia danych powinna również uwzględniać sytuacje, w których nośniki danych służące do przetwarzania informacji Podmiotu nadzorowanego będą utylizowane lub wykorzystywane wtórnie do innych celów.

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.5.17. **Załącznik nr 6** – Kwestionariusz - okresowe monitorowanie umów.

5.5.18. **Załącznik nr 13** – Objaśnienia i lista wybranych klauzul wraz z przykładami.

5.6. PLAN PRZETWARZANIA INFORMACJI W CHMURZE OBLICZENIOWEJ

5. Plan przetwarzania informacji w chmurze obliczeniowej

5.1 Podmiot nadzorowany na podstawie wyników szacowania ryzyka opracowuje udokumentowany plan przetwarzania informacji w chmurze obliczeniowej, który zawiera co najmniej:

a) rodzaj (opis) przetwarzanych informacji oraz informację, jeżeli stosowane, o ich pseudonimizacji lub anonimizacji;

b) sposób szyfrowania informacji oraz miejsce (lub sposób) zarządzania kluczami szyfrującymi;

c) informację o tym, kto ma dostęp do przetwarzanych informacji oraz jak ten dostęp jest nadawany, zarządzany, odbierany oraz kontrolowany;

d) datę zawarcia umowy z dostawcą usług chmury obliczeniowej i referencje do tej umowy (numer, okres obowiązywania, datę przedłużenia lub zmiany, daty rozpoczęcia korzystania z usług), a w przypadku, gdy umowa nie jest jeszcze zawarta – przewidywaną datę jej zawarcia;

e) prawo właściwe, któremu podlega umowa;

f) opis zadania realizowanego za pomocą usługi chmury obliczeniowej wraz z informacją, czy jest to outsourcing szczególny chmury obliczeniowej w rozumieniu niniejszego komunikatu lub czy przetwarzane są informacje prawnie chronione.

OPIS WYMAGAŃ

5.6.1. Podmiot nadzorowany w ramach bieżącego i planowanego przetwarzania informacji w Chmurze obliczeniowej powinien posiadać udokumentowany plan przetwarzania informacji w Chmurze obliczeniowej. Szablon planu przetwarzania informacji w chmurze obliczeniowej znajduje się w Załączniku nr 14 do Modelu. Plan ten w szczególności powinien zawierać:

1) opis zadania realizowanego za pomocą Usługi chmury obliczeniowej;

2) rodzaj (chronione, niechronione), klasę (publiczne, wewnętrzne, poufne) i typ (produkcyjne, testowe) przetwarzanych informacji, ze wskazaniem czy przetwarzanie spełnia kryteria Outsourcingu szczególnego chmury obliczeniowej;

3) mechanizmy zabezpieczenia informacji (pseudonimizacja, anonimizacja), mechanizmy szyfrowania informacji, w tym zasady zarządzania i przechowywania kluczy szyfrujących oraz opis kontroli dostępu do informacji.

5.6.2. Plan powinien precyzyjnie określić jakie dane (informacje) Podmiot nadzorowany, w ramach konkretnej inicjatywy, przetwarza w Chmurze obliczeniowej.

5.6.3. Zgodnie z pkt. VII. A. 3. – plan powinien być przeglądany w ustalonych cyklach bądź przy wystąpieniu większych zmian w zakresie lub sposobie przetwarzania informacji w Chmurze Obliczeniowej

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.6.4. Udokumentowany Plan przetwarzania informacji w chmurze obliczeniowej dla danej usługi.

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.6.5. Brak

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.6.6. **Załącznik nr 14** – „Plan Przetwarzania informacji w chmurze obliczeniowej”.

5.7. TESTY

5.2. **[Testy]** Uruchomienie produkcyjne stosowania usług chmury obliczeniowej powinien poprzedzać okres testowy, podczas którego na danych testowych (generowanych maszynowo lub w inny przypadkowy sposób), w udokumentowanym procesie, testowane są scenariusze adekwatne do oszacowanego ryzyka.

OPIS WYMAGAŃ

5.7.1. Podmiot nadzorowany powinien przeprowadzić i udokumentować fazę testów usługi. Testy powinny być przeprowadzone na danych testowych; scenariusze testów powinny być adekwatne do oszacowanego ryzyka (zgodnie z rozdziałem VI Komunikatu - Wytyczne do szacowania ryzyka).

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.7.2. Udokumentowane scenariusze testowe dla danej usługi.

5.7.3. Formalne wyniki testów dla danej usługi.

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.7.4. Brak

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.7.5. Brak

5.8. PLAN WYCOFANIA

5.3 **[Plan wycofania]** Podmiot nadzorowany posiada udokumentowany, przetestowany plan wycofania swojego zaangażowania w przetwarzanie informacji w usługach chmury obliczeniowej danego dostawcy (również w sytuacji awaryjnej), bez uszczerbku dla zachowania zgodności swojego działania z wymaganiami prawa i innych regulacji, w tym w szczególności związanych z udzielonymi licencjami lub zezwoleniami na prowadzenie określonej działalności.

OPIS WYMAGAŃ

5.8.1. Podmiot nadzorowany posiada plan wycofania się z Usługi chmury obliczeniowej zarówno w sytuacji zmiany strategii, jaki w sytuacji awaryjnej.

5.8.2. Plan wycofania powinien zapewnić, że w sytuacji awaryjnej nie dojdzie do uszczerbku dla zachowania zgodności działania Podmiotu nadzorowanego z wymaganiami prawa i z innymi regulacjami, w tym związanymi z udzielonymi licencjami lub zezwoleniami na prowadzenie określonej działalności.

5.8.3. Plan wycofania powinien być adekwatny do oszacowanego ryzyka, skali, krytyczności danych i procesu uruchomionego w chmurze obliczeniowej lub w oparciu o Chmurę obliczeniową. W szczególności, Podmiot nadzorowany opracowując plan wycofania może zastosować podejście oparte o analizę procesów i wykorzystywanych Usług, biorąc pod uwagę, (z uwzględnieniem VI.2.1.e. i h. Komunikatu), które z tych procesów i rozwiązań mają istotny wpływ na działalność Podmiotu nadzorowanego (jak np. lista procesów istotnych/krytycznych).

5.8.4. Plan wycofania się z usługi może zakładać powrót do środowiska on-premises, migrację do innego Dostawcy lub inne uzasadnione biznesowo scenariusze.

5.8.5. Plan wycofania może bazować na ogólnodostępnych informacjach technicznych dotyczących danego rozwiązania.

5.8.6. Plan powinien być przetestowany, przy czym zakres i podejście do testów powinny wynikać z analizy ryzyka (zgodnie z rozdziałem VI Komunikatu - Wytyczne do szacowania ryzyka) i uwzględniać takie kwestie jak wolumeny danych, wymagane zasoby, etc. Dokumentacja testowa powinna zawierać odpowiednie dowody audytowe, np. scenariusze testowe, oczekiwane wyniki, logi czy zrzuty z ekranu, potwierdzające fakt przeprowadzenia testów zgodnie z założeniami. Testy planu wycofania powinny w szczególności:

1) obejmować procesy i rozwiązania, które mają istotny wpływ na działalność Podmiotu nadzorowanego, a nie Dostawcę usług chmury obliczeniowej;

2) być zrealizowane praktycznie poprzez rzeczywiste wykonanie określonych w scenariuszach kroków.

5.8.7. Rekomendowane jest także cykliczne testowanie planu wycofania, w oparciu o różne procesy mające istotny wpływ na Podmiot nadzorowany oraz różne rozwiązania. Rekomendowane jest także aktualizacja i przetestowanie planu wycofania w razie istotnych zmian w korzystaniu z usług chmury obliczeniowej mających wpływ na wycofanie

z przetwarzania w chmurze – jak np. w razie uruchomienia kolejnego procesu biznesowego w oparciu o te same usługi. Zasady aktualizacji powinny być opisane w wewnętrznych procedurach. Rekomenduje się testowanie planu wycofania nie rzadziej niż raz w roku.

5.8.8. Plan wycofania powinien zawierać kryteria podjęcia decyzji o uruchomieniu planu wycofania się z Usługi chmury obliczeniowej, takie jak w szczególności:

1) nieakceptowalna zmiana warunków świadczenia usługi przez Dostawcę (jak np. wykorzystanie nieakceptowalnego poddostawcy, obniżenie SLA);
2) wypowiedzenia umowy przez Dostawcę;
3) decyzja biznesowa o zaprzestaniu korzystania z Usługi;
4) decyzja administracyjna nakazująca Podmiotowi nadzorowanemu rozwiązanie umowy z Dostawcą.

5.8.9. Podmiot nadzorowany powinien zadbać o odpowiednie wymagania certyfikowanego usunięcia danych zgodnie z opisem wymagań dla Umowy z dostawcą usług chmury obliczeniowej (ppkt 4.1.q) Komunikatu).

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.8.10. Plan wycofania się z danej Usługi chmury obliczeniowej.

5.8.11. Scenariusze testowe i wyniki testów dla planu wycofania się z Usługi chmury obliczeniowej w związku z zakończeniem umowy.

5.8.12. Scenariusze testowe i wyniki testów dla planu wycofania się z Usługi chmury obliczeniowej w związku z sytuacją awaryjną.

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.8.13. Procedura lub wzór certyfikatu, potwierdzające skuteczne usunięcie danych zgodnie z opisem pkt. 5.8.9.

5.8.14. Umowa z dostawcą usług chmury obliczeniowej, ppkt 4.1.q) Komunikatu.

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.8.15. **Załącznik nr 15** – Szablon scenariusza wyjścia z relacji z Dostawcą.

5.8.16. **Załącznik nr 16** – Wyjście z chmury – główne zagadnienia.

5.9. PLAN CIĄGŁOŚCI DZIAŁANIA

5.4 **[Plan ciągłości działania]** Podmiot nadzorowany powinien posiadać udokumentowany plan ciągłości działania uwzględniający możliwość utraty kontroli nad przetwarzanymi informacjami u danego dostawcy usług chmury obliczeniowej oraz możliwość przerwania ciągłości działania usługi. W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej chmur obliczeniowych lub dwóch lub więcej dostawców usług chmury obliczeniowej, podmiot nadzorowany regularnie weryfikuje własną zdolność do utrzymania deklarowanych założeń, w szczególności zgodność konfiguracji usług i odtwarzalności środowiska teleinformatycznego, zwłaszcza po zmianach technologicznych u jednego z dostawców usług chmury obliczeniowej.

OPIS WYMAGAŃ

5.9.1. Podmiot nadzorowany powinien rozszerzyć posiadane plany ciągłości działania o scenariusz uwzględniający potencjalną możliwość utraty kontroli nad przetwarzanymi informacjami u danego Dostawcy oraz możliwość przerwania ciągłości działania Usługi chmury obliczeniowej.

5.9.2. Plan ciągłości działania może być oparty na różnych scenariuszach, w szczególności zakładać wykorzystanie środowiska on-premise, wykorzystanie innego Dostawcy, lub tymczasową alternatywną realizację procesów (np. manualnie).

5.9.3. Podmiot nadzorowany może polegać na planach ciągłości działania po stronie Dostawcy pod warunkiem posiadania nadzoru nad działaniami Dostawcy w tym zakresie, tj. regularnej weryfikacji adekwatności planu oraz wyników testów planu ciągłości działania i planów awaryjnych (np. poprzez weryfikacje wyników niezależnych audytów, certyfikacje, etc.).

5.9.4. W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej Chmur obliczeniowych lub dwóch lub więcej Dostawców, Podmiot nadzorowany powinien regularnie weryfikować możliwość realizacji tego scenariusza, zwłaszcza po zmianach technologicznych u jednego z Dostawców.

5.9.5. W przypadku SaaS, gdy Dostawca usługi chmury obliczeniowej wykorzystuje zewnętrzną chmurę obliczeniową swojego poddostawcy, może być konieczne zaangażowanie poddostawcy w tworzeniu planu ciągłości działania, niezależnie od tego, że nie jest nawiązana z nim relacja umowna. UKNF zwraca uwagę, że w przypadku łańcucha outsourcingowego przewidzianego w rozdziale VI pkt 2 ppkt 7 Komunikatu, ryzyko związane z ciągłością działania związane jest z funkcjonowaniem dwóch podmiotów: Dostawcy usługi i poddostawcy chmury obliczeniowej. Plan ciągłości działania, jakkolwiek możliwy do ujęcia w jednym dokumencie, powinien zatem obejmować przypadki utraty kontroli nad przetwarzanymi informacjami jako efekt zaistnienia zdarzeń dotyczących działalności Dostawcy, jak i jego poddostawcy chmury obliczeniowej. Powinien również uwzględniać sposób działania w przypadku jednoczesnego wystąpienia negatywnych zdarzeń po stronie obu tych podmiotów, co jest możliwe np. w sytuacji, kiedy oba podmioty należą do jednej grupy kapitałowej.

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.9.6. Plan ciągłości działania dla Usługi chmury obliczeniowej, zawierający jako minimum opisane procesy i procedury w sytuacjach:

1) możliwości utraty kontroli nad przetwarzanymi informacjami u danego Dostawcy;

2) możliwości przerwania ciągłości działania Usługi chmury obliczeniowej.

5.9.7. Dokumentacja związana z Planowaniem Ciągłości Działania zgodnie z metodyką przyjętą w Podmiocie nadzorowanym (zawierająca w szczególności wyniki testów ciągłości działania).

5.9.8. W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej Chmur obliczeniowych lub dwóch lub więcej Dostawców:

1) dokumentacja weryfikacji możliwości realizacji tego scenariusza, np. przeprowadzenie testowej migracji próbki danych lub usług pomiędzy dwoma Usługami chmury obliczeniowej;

2) potwierdzenie przeprowadzania okresowej weryfikacji możliwości realizacji scenariusza z podpunktu powyżej, w szczególności dotycząca weryfikacji możliwości realizacji scenariusza po zmianach technologicznych u jednego z Dostawców.

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.9.9. Plan ciągłości działania.

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.9.10. Brak

5.10. WYMAGANIA DLA DOSTAWCÓW USŁUG CHMURY OBLICZENIOWEJ

6. Wymagania dla dostawców usług chmury obliczeniowej

6.1 W zakresie świadczonych usług chmury obliczeniowej i odpowiednio do ich skali dostawca usług chmury obliczeniowej spełnia wymagania zapewnienia zgodności swojego działania z poniższymi normami lub ich odpowiednikami w polskim lub europejskim układzie normalizacji, chyba że podmiot nadzorowany akceptuje (na podstawie wyników szacowania ryzyka) brak konieczności spełnienia tego wymagania albo jego części:

a) PN-ISO/IEC ISO 20000 dotyczące zarządzania usługami IT;

b) PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji;

c) PN-EN ISO 22301 dotyczące zarządzania ciągłością działania;

d) ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze obliczeniowej;

e) ISO/IEC 27018 dotyczące dobrych praktyk zabezpieczania danych osobowych w chmurze obliczeniowej.

6.2 CPD dostawcy usług chmury obliczeniowej spełnia wymagania normy PN-EN 50600 (Wyposażenie i infrastruktura centrów przetwarzania danych) minimum klasy 3 lub ANSI/TIA-942 minimum Tier III, lub innego normatywu odpowiedniego i uznanego do oceny CPD lub zawierającego wymagania z nim związane, przy czym podmiot nadzorowany może zaakceptować (w uzasadnionych przypadkach i na podstawie szacowania ryzyka) brak spełnienia części wymagań.

6.3 Spełnienie wymagań może być poświadczone odpowiednimi certyfikatami zgodności wystawionym przez niezależne jednostki certyfikujące, akredytowane w polskim lub europejskim systemie akredytacji.

OPIS WYMAGAŃ

5.10.1. Podmiot nadzorowany, w zależności od oceny ryzyka, podejmuje decyzję o konieczności częściowego lub pełnego spełnienia przez Dostawcę:

1) wskazanych w Komunikacie norm ISO;

2) wymagań w zakresie CPD.

5.10.2. Podmiot nadzorowany akceptując odstępstwa od spełnienia wymogów wskazanych w Komunikacie norm, powinien udokumentować motywy takiego podejścia np. poprzez wskazanie, że zaakceptowane przez Podmiot nadzorowany CPD spełnia inne wymogi. W przypadku SaaS, powyższe wymagania dotyczą zarówno Dostawcy usługi chmury obliczeniowej, jak i jego poddostawcy w zakresie infrastruktury chmury obliczeniowej, do którego stosowały się będą w szczególności wymogi dotyczące CPD.

5.10.3. Zakres w/w wymagań dla każdego wdrożenia powinien być przez Podmiot nadzorowany udokumentowany.

5.10.4. W zależności od decyzji Podmiotu nadzorowanego, Dostawca powinien zobowiązać się w umowie do zapewnienia zgodności Usługi chmury obliczeniowej z w/w normami lub ich odpowiednikami (normami BS, normami PN-ISO, etc.).

5.10.5. Zapewnienie zgodności może być realizowane poprzez uzyskanie przez Dostawcę niezależnej certyfikacji (wydanej przez jednostkę certyfikującą); w przypadku, gdy Dostawca nie posiada formalnej certyfikacji, powinien on wykazać zgodność z w/w normami poprzez udokumentowanie realizacji poszczególnych wymagań norm.

5.10.6. Zakres certyfikacji powinien obejmować w całości usługę świadczoną na rzecz Podmiotu nadzorowanego, w szczególności zgodnie z pkt. 6.2 fragmentu Komunikatu cytowanego powyżej, wszystkie CPD w których przetwarzane są dane (informacje) Podmiotu nadzorowanego.

5.10.7. Dokumentacja związana z certyfikacją tj. certyfikat oraz wyniki audytów certyfikacyjnych lub dokumentacja zgodności dostarczona przez Dostawcę, powinny być przekazane przed zawarciem umowy oraz co najmniej raz w roku udostępniane Podmiotowi nadzorowanemu.

5.10.8. Podmiot nadzorowany powinien regularnie weryfikować dokumentację związaną z certyfikacją; w przypadku, gdy w/w dokumentacja wykaże istotne niezgodności, Podmiot nadzorowany powinien uzgodnić z Dostawcą plan naprawczy oraz monitorować jego realizację.

5.10.9. Aby w kompletny sposób podejść do oceny Dostawcy rozwiązania bazującego na usłudze chmurowej w kontekście wymagań Komunikatu chmurowego, w Załączniku nr 8 „Ankieta dla dostawców usługi chmurowej" oraz Załączniku nr 9 „Ankieta dla dostawców – udokumentowanie konfiguracji usługi" zaproponowano listę pytań, które należy uzgodnić z planowanym dostawcą rozwiązania, aby potwierdzić gotowość proponowanego rozwiązania/usługi w kontekście wspomnianych wymagań, a z którymi zgodność m.in. będzie musiał wykazać Podmiot nadzorowany przed UKNF, w celu uruchomienia przetwarzania chmurowego w ramach tego rozwiązania/usługi.

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.10.10. Udokumentowane wymagania Podmiotu nadzorowanego w zakresie norm i standardów, w szczególności dokumentacja akceptacji ryzyka w przypadku rezygnacji z wymagań.

5.10.11. Pozyskanie certyfikatu od Dostawcy lub innej dokumentacji zgodności Dostawcy z normami.

5.10.12. Udokumentowany proces regularnej oceny dokumentacji związanej z certyfikacją/zgodnością.

5.10.13. Udokumentowany proces zarządzania planami naprawczymi uzgodnionymi z Dostawcą w przypadku istotnych niezgodności z normami.

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.10.14. Certyfikacja zgodnie z w/w normami, obejmująca zakresem usługę świadczoną na rzecz Podmiotu nadzorowanego lub dokumentacja zgodności z w/w normami przygotowana przez Dostawcę Dokumenty certyfikacji oraz dokumentacja zgodności z w/w normami powinny być integralną częścią umowy podpisywanej z Podmiotem nadzorowanym.

5.10.15. Wymogi dotyczące certyfikacji powinny obejmować również poddostawców w sytuacji, kiedy w ich CPD przetwarzane są dane (informacje) Podmiotu nadzorowanego.

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.10.16. **Załącznik nr 8** – Ankieta dla dostawców usługi chmurowej.

5.10.17. **Załącznik nr 9** – Ankieta dla dostawców – udokumentowanie konfiguracji usługi.

5.10.18. **Załącznik nr 17** – Szablon dokumentacji kontroli ISO27001.

5.10.19. **Załącznik nr 18** – Lista zagadnień dla wyboru dostawców związanych z bezpieczeństwem.

5.11. LOKALIZACJA CPD

6.3 **[Lokalizacja CPD]** Nadzór rekomenduje, aby CPD zlokalizowane było na terytorium państwa Europejskiego Obszaru Gospodarczego (EOG). Punkt ten stosuje się z zastrzeżeniem, że podmioty nadzorowane, które:

a) zostały uznane stosowną decyzją za operatorów usług kluczowych w rozumieniu art. 5 ust. 2 ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa i którzy wykorzystują usługę chmury obliczeniowej w zakresie realizacji usługi kluczowej lub

b) są operatorami infrastruktury krytycznej w rozumieniu ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym i którzy wykorzystują usługę chmury obliczeniowej w zakresie realizacji zadań operowania infrastrukturą krytyczną

- powinny w pierwszej kolejności wykorzystywać CPD znajdujące się na terenie Rzeczypospolitej Polskiej, o ile – w ocenie podmiotu nadzorowanego – oferowane warunki umowne, ekonomiczne, operacyjne, SLA czy funkcjonalne są nie gorsze od CPD znajdujących się poza terytorium Rzeczypospolitej Polskiej.

OPIS WYMAGAŃ

5.11.1. Rekomendowany jest wybór Dostawców oferujących CPD na terenie EOG, co nie wyklucza możliwości przetwarzania danych (informacji) przez Dostawcę poza EOG.

5.11.2. Jeżeli usługa ma być świadczona w CPD na terenie EOG (lub w Polsce zgodnie pkt. 6.3. fragmentu Komunikatu cytowanego powyżej), Podmiot nadzorowany korzystający z usług globalnego Dostawcy powinien zdefiniować mechanizmy kontrolne zapewniające, że usługi, które wykorzystuje są świadczone w CPD na terenie EOG (lub w Polsce zgodnie z pkt 6.3. fragmentu Komunikatu cytowanego powyżej).

5.11.3. Podmioty będące operatorami infrastruktury krytycznej lub będące operatorami usługi kluczowej, powinny preferować CPD znajdujące się na terenie Polski, o ile oferuje ono nie gorsze warunki (bezpieczeństwo, koszt, SLA, itp.) niż usługi zlokalizowane poza Polską. W związku z tym, Podmioty nadzorowane będące w/w operatorami powinny przed wyborem Dostawcy zweryfikować dostępność analogicznej usługi korzystającej z CPD w Polsce i zapewnić udokumentowane porównanie tych usług – w szczególności porównując (szacując zgodnie z Komunikatem) ryzyko i koszty dla poszczególnych wariantów.

5.11.4. Podmiot nadzorowany powinien, nie rzadziej niż raz w roku, weryfikować, czy usługa chmury obliczeniowej lub przetwarzane dane (informacje) nie są przetwarzane w CPD zlokalizowanym w innym regionie niż w momencie rozpoczęcia dostarczania usługi chmury obliczeniowej lub przetwarzania danych (informacji) w chmurze obliczeniowej, przy czym wystarczające jest tu oświadczenie Dostawcy.

5.11.5. Podmiot nadzorowany powinien zapewnić sobie prawo rozwiązania umowy na usługę chmury obliczeniowej na wypadek niezgodnej z umową zmiany lokalizacji CPD w którym przetwarzane są dane Podmiotu nadzorowanego.

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.11.6. Jednoznaczne wskazanie lokalizacji CPD wykorzystywanych w usłudze. Jeżeli poszczególne usługi chmury obliczeniowej Dostawcy zlokalizowane są w różnych lokalizacjach CPD, należy wskazać lokalizację dla każdej z nich.

5.11.7. Dla operatorów infrastruktury krytycznej lub operatorów usługi kluczowej - dokumentacja lub mechanizmy kontrolne potwierdzające lokalizacje CPD w Polsce (jeśli dotyczy).

5.11.8. W przypadku, gdy uzasadniony jest wybór CPD poza EOG (lub poza Polską, zgodnie z pkt. 6 Wymagania dla dostawców usług chmury obliczeniowej, ppkt 6.3. Komunikatu), udokumentowana analiza uzasadniająca taką decyzję (kwestie kosztów, ryzyka, operacyjne i/lub funkcjonalne lub ryzyka).

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.11.9. Jednoznaczne wskazanie wszystkich lokalizacji CPD (kraj/region) wykorzystywanych w poszczególnych usługach (w formie oświadczenia Dostawcy).

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.11.10. Brak

5.12. DOSTĘP DO PRZETWARZANYCH INFORMACJI

6.4 **[Dostęp do przetwarzanych informacji]** Dostawca usług chmury obliczeniowej zapewnia w swoim postępowaniu udokumentowaną zasadę ochrony przetwarzanych przez podmiot nadzorowany informacji przed nieautoryzowanym dostępem lub użyciem przez swoich pracowników lub poddostawców poprzez co najmniej:

a) domyślną zasadę braku dostępu do przetwarzanych informacji podmiotu nadzorowanego;

b) domyślną zasadę braku konta administracyjnego lub użytkownika na maszynach wirtualnych podmiotu nadzorowanego lub w innych uruchamianych usługach chmury obliczeniowej;

c) zasadę „minimum koniecznego" dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez podmiot nadzorowany (w tym również usunięcia usterek) oraz na czas ich trwania, przy czym realizacja czynności poprzedzona jest zleceniem podmiotu nadzorowanego, a cały proces obsługi i wykonania czynności jest logowany. Obowiązujące w tym zakresie procedury obsługi mogą być dodatkowo potwierdzone stosownym certyfikatem (np. SOC 2 Type 2) wydanym przez niezależną jednostkę certyfikującą akredytowaną w europejskim systemie akredytacji;

d) udostępnienie wytycznych, wzorcowych konfiguracji, opisów zasad, itp., które w jednoznaczny sposób definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji;

e) domyślne uruchamianie nowego środowiska (lub usługi chmury obliczeniowej) separowanego od innych tenantów, z ustawieniami „secure-by-default".

OPIS WYMAGAŃ

5.12.1. Dostawca powinien przedstawić dokumentację mechanizmów kontroli dostępu do danych (informacji) przetwarzanych w Usłudze chmury obliczeniowej, w tym dla swoich pracowników (współpracowników) i poddostawców.

5.12.2. Dostawca nie powinien mieć stałego dostępu administracyjnego i serwisowego na poziomie urządzeń (serwerów, switchy, macierzy dyskowych, etc.) ani oprogramowania stanowiącego element dostarczanej usługi dla Podmiotu nadzorowanego (platformy chmury obliczeniowej, baz danych, aplikacji, etc.). Wszelkie czynności administracyjne i serwisowe powinny być logowane i audytowane.

5.12.3. Dostawca domyślnie nie powinien mieć żadnego dostępu do danych (informacji).

5.12.4. Dostawca powinien zagwarantować Podmiotowi nadzorowanemu odpowiednie mechanizmy kontroli i limitowanie praw dostępu jak opisane powyżej w odniesieniu do swoich poddostawców.

5.12.5. Dostęp do danych (informacji) dla Dostawcy powinien być nadawany tymczasowo na podstawie udokumentowanego żądania powiązanego z konkretnymi pracami administracyjnymi, rozwojowymi lub wsparciem użytkowników (zleconymi przez Podmiot nadzorowany).

5.12.6. Dostawca powinien przekazać dokumentację potwierdzającą separację tenantów oraz dokumentację mechanizmów zapewniających poprawność separacji, tak aby możliwa była okresowa weryfikacja konfiguracji. Separacja powinna być realizowana co najmniej na poziomie logicznym – na poziomie odpowiednich konfiguracji logicznych i uprawnień na platformie chmury obliczeniowej Dostawcy, bez możliwości dostępu do zasobów przynależnych do innych tenantów.

5.12.7. Nowo uruchamiane środowiska i/lub usługi powinny być domyślnie odseparowane od innych tenantów korzystających z chmury obliczeniowej Dostawcy (od momentu uruchomienia) i skonfigurowane zgodnie z najlepszymi praktykami bezpieczeństwa (hardening).

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.12.8. Dokumentacja mechanizmów kontroli dostępu, przy założeniu, że jako minimum przyjęto:

1) potwierdzenie domyślnego braku dostępu do danych (informacji), kont administracyjnych, serwisowych etc.;
2) opis mechanizmów nadawania dostępu administracyjnego.

5.12.9. Potwierdzenie zasady „minimum koniecznego” przy dostępie serwisowym.

5.12.10. Dokumentacja mechanizmów separacji danych (informacji):

1) wytycznych, wzorcowych konfiguracji, opisów zasad, itp., które w jednoznaczny sposób definiują separację przetwarzania;
2) wytycznych, wzorcowych konfiguracji, opisów zasad weryfikacji poprawności konfiguracji.

5.12.11. Dokumentacja konfiguracji bezpieczeństwa nowo uruchamianych serwerów i usług („secure-by-default”).

5.12.12. Opcjonalnie, certyfikaty i dokumentacja certyfikacji (wyniki audytu, itp.) w zakresie funkcjonowania mechanizmów kontroli dostępu.

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.12.13. Dostawca usług chmury obliczeniowej zapewnia w swoim postępowaniu udokumentowaną zasadę ochrony przetwarzanych przez podmiot nadzorowany informacji przed nieautoryzowanym dostępem lub użyciem przez swoich pracowników lub poddostawców poprzez co najmniej:

1) domyślną zasadę braku dostępu do przetwarzanych informacji podmiotu nadzorowanego;

2) domyślną zasadę braku konta administracyjnego lub użytkownika na maszynach wirtualnych podmiotu nadzorowanego lub w innych uruchamianych usługach chmury obliczeniowej;

3) zasadę „minimum koniecznego" dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez Podmiot nadzorowany (w tym również usunięcia usterek) oraz na czas ich trwania, przy czym realizacja czynności poprzedzona jest zleceniem podmiotu nadzorowanego, a cały proces obsługi i wykonania czynności jest logowany. Obowiązujące w tym zakresie procedury obsługi mogą być dodatkowo potwierdzone stosownym certyfikatem (np. SOC 2 Type 2) wydanym przez niezależną jednostkę certyfikującą akredytowaną w europejskim systemie akredytacji;

4) udostępnienie wytycznych, wzorcowych konfiguracji, opisów zasad, itp., które w jednoznaczny sposób definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji;

5) domyślne uruchamianie nowego środowiska (lub usługi chmury obliczeniowej) separowanego od innych tenantów, z ustawieniami „secure-by-default".

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.12.14. **Załącznik nr 8** – Ankieta dla dostawców usługi chmurowej.

5.12.15. **Załącznik nr 9** – Ankieta dla dostawców – udokumentowanie konfiguracji usługi.

5.13. KRYPTOGRAFIA

7.1. Podmiot nadzorowany powinien zapewnić, że informacje przetwarzane w chmurze obliczeniowej są szyfrowane zgodnie z zasadami określonymi w niniejszym komunikacie. W szczególności podmiot nadzorowany powinien upewnić się, że:

a) posiada dostęp do szczegółowych i aktualnych instrukcji konfiguracji usług chmury obliczeniowej oraz metod weryfikacji poprawności ich konfiguracji i działania, w szczególności w zakresie szyfrowania przetwarzanych informacji;

b) zapewnia dostateczne kompetencje w celu realizacji poprawnej konfiguracji usług chmury obliczeniowej, zgodnie z wytycznymi dostawcy usług chmury obliczeniowej, w tym pod kątem stosowania szyfrowania przetwarzanych informacji;

c) używa dedykowanych lub zalecanych przez dostawcę usług chmury obliczeniowej ustawień konfiguracyjnych podnoszących bezpieczeństwo świadczonych usług chmury obliczeniowej;

d) informacje prawnie chronione przetwarzane w chmurze obliczeniowej są szyfrowane zarówno „at rest" jak i „in transit".

OPIS WYMAGAŃ

5.13.1. Wymagane jest szyfrowanie informacji przetwarzanych w Chmurze obliczeniowej. Mechanizmy i zakres wykorzystywania zabezpieczeń kryptograficznych powinien wynikać z analizy ryzyka (zgodnie z rozdziałem VI pkt 2. ppkt 5 z ustępami, Komunikatu). W szczególności wymagane jest:

1) szyfrowanie, zarówno podczas przesyłu jak i podczas spoczynku („at rest" jak i „in transit") danych objętych Tajemnicą zawodową;

2) przekazanie Podmiotowi nadzorowanemu przez Dostawcę dokumentacji mechanizmów szyfrowania danych (informacji), a także mechanizmów weryfikacji poprawności konfiguracji i działania w/w mechanizmów;

3) posiadanie przez Podmiot nadzorowany kompetencji w zakresie poprawnej konfiguracji usług, w tym mechanizmów szyfrowania;

4) korzystanie przez Podmiot nadzorowany z zalecanych ustawień podnoszących bezpieczeństwo (tzw. hardening); ustawienia te powinny zostać udokumentowane.

5.13.2. Aby ułatwić Podmiotom nadzorowanym i Dostawcom usług chmurowych odpowiednie przygotowanie kwestii dotyczących kryptografii, można skorzystać z listy pytań zawartych w Załączniku nr 19 „Kryptografia", które Podmiot nadzorowany powinien sobie zadać w celu oceny kompletności/gotowości tego aspektu bezpieczeństwa dla planowanego/realizowanego przetwarzania chmurowego w ramach usługi.

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.13.3. Udokumentowane potwierdzenie dostępu do instrukcji konfiguracji usług chmury obliczeniowej oraz metod weryfikacji poprawności ich konfiguracji i działania.

5.13.4. Udokumentowane potwierdzenie kompetencji w obszarze realizacji poprawnej konfiguracji zgodnie z wytycznymi dostawcy usługi chmurowej.

5.13.5. Udokumentowane potwierdzenie używanych ustawień konfiguracyjnych dla danej usługi.

5.13.6. Udokumentowane potwierdzenie, że informacje prawnie chronione przetwarzane w danej usłudze są szyfrowane zarówno „at rest" jak i „in transit".

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.13.7. Dokumentacja mechanizmów szyfrowania oraz metody weryfikacji poprawności konfiguracji szyfrowania.

5.13.8. Potwierdzenie posiadanych kompetencji – patrz rozdział VII pkt 3 Komunikatu.

5.13.9. Dokumentacja hardeningu usługi, w szczególności mechanizmów szyfrowania.

5.13.10. Potwierdzenie szyfrowania danych (informacji) w spoczynku i podczas przesyłu (dokumentacja techniczna, zrzuty ekranu, etc.).

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.13.11. **Załącznik nr 19** – Kryptografia.

5.14. KRYPTOGRAFIA C.D.

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.

[…]

7.4 Podmiot nadzorowany w udokumentowanym procesie zarządza tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących oraz kontrolą tego procesu.

7.5 Proces zarządzania kluczami szyfrującymi powinien uwzględniać przechowywanie w ramach własnej infrastruktury kopii kluczy szyfrujących, które zostały wygenerowane lub są zarządzane przez dostawcę usług chmury obliczeniowej i są używane w procesie outsourcingu szczególnego chmury obliczeniowej, chyba że z oszacowania ryzyka wynika uzasadniony brak takiej potrzeby.

OPIS WYMAGAŃ

5.14.1. Podmiot nadzorowany powinien zapewnić, że informacje są szyfrowane kluczami generowanymi oraz zarządzanymi przez Podmiot nadzorowany. Brak spełnienia tego wymogu powinien zostać poparty stosowną analizą ryzyka (patrz rozdział VII pkt 7. ppkt 7.2 Komunikatu).

5.14.2. Proces zarządzania tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących powinien być udokumentowany i posiadać określone mechanizmy kontrolne.

5.14.3. W przypadku wykorzystania kluczy wygenerowanych lub zarządzanych przez Dostawcę, Podmiot nadzorowany powinien zapewnić, że proces wspomniany w pkt. 5.14.2 powyżej zapewnia przechowywanie kluczy w infrastrukturze Podmiotu nadzorowanego, chyba że analiza ryzyka dopuszcza brak takiego mechanizmu.

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.14.4. Dokumentacja techniczna potwierdzająca, że informacje są szyfrowane kluczami generowanymi lub dostarczonymi oraz zarządzanymi przez Podmiot nadzorowany.

5.14.5. W przypadku, gdy pkt 5.14.4 powyżej nie jest spełniony, analiza ryzyka z której wynika dopuszczalność używania kluczy szyfrujących generowanych/dostarczonych i zarządzanych przez Dostawcę.

5.14.6. Sformalizowany (udokumentowany) proces (procedura) zarządzania tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących oraz przechowywaniem kopii zapasowych kluczy w infrastrukturze Podmiotu nadzorowanego.

5.14.7. W przypadku gdy proces zarządzania kluczami szyfrującymi nie zapewnia przechowywania kopii kluczy w infrastrukturze Podmiotu nadzorowanego, analiza ryzyka z której wynika dopuszczalny brak takiej potrzeby.

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.14.8. Opis procedur i mechanizmów zarządzania kluczami szyfrującymi, sformalizowany (udokumentowany) proces zarządzania tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących.

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.14.9. Załącznik 7. Wymagania dla dostawców usług chmurowych zgodnie z Komunikatem.

5.14.10. Załącznik 19. – Kryptografia.

5.15. KRYPTOGRAFIA C.D.

	7.3 W przypadku, gdy z szacowania ryzyka wynika konieczność utrzymywania i zarządzania kluczami szyfrującymi przy wykorzystaniu sprzętowych rozwiązań (HSM), to HSM mogą być udostępniane przez dostawcę usług chmury obliczeniowej, przy uwzględnieniu tego elementu w szacowaniu ryzyka. HSM powinny spełniać wymagania minimum FIPS 140 2 Level 2 lub równoważne.

OPIS WYMAGAŃ

5.15.1. W zależności od wyników analizy ryzyka (rozdział VI Komunikatu, Wytyczne do szacowania ryzyka, pkt 2. ppkt. 5. z ustępami) możliwe jest stosowanie HSM. HSM może być udostępniony przez Dostawcę lub być zarządzany przez Podmiot nadzorowany. Bez względu na to, która strona udostępnia HSM, musi on spełniać wymagania FIPS 140-2 Level 2 lub równoważne.

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.15.2. Odniesienie się do wymogu dotyczącego HSM w analizie ryzyka.

5.15.3. W przypadku wykorzystania HSM - dokumentacja wykorzystywanych HSM potwierdzająca spełnienie wymagania FIPS 140-2 Level 2 lub równoważnego (w szczególności FIPS 140-3, który jest następcą wymagań FIPS 140-2).

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.15.4. Jak wyżej w pkt 5.15.3, w przypadku, gdy HSM jest udostępniony przez Dostawcę.

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.15.5. Załącznik 7. Wymagania dla dostawców usług chmurowych zgodnie z Komunikatem.

5.15.6. Załącznik 19. – Kryptografia..

5.16. MONITOROWANIE ŚRODOWISKA PRZETWARZANIA INFORMACJI W USŁUGACH CHMURY OBLICZENIOWEJ

8. Monitorowanie środowiska przetwarzania informacji w usługach chmury obliczeniowej

8.1 Podmiot nadzorowany posiada udokumentowane zasady zbierania logów związanych z przetwarzaniem informacji w chmurze obliczeniowej, stosownie do zakresu używanych usług chmury obliczeniowej, przetwarzanych informacji i wyników szacowania ryzyka.

8.2 Podmiot nadzorowany zabezpiecza logi przed nieautoryzowanym dostępem, modyfikacją lub usunięciem przez okres zgodny z ustalonymi zasadami bezpieczeństwa wynikającymi z szacowania ryzyka oraz obowiązującymi przepisami szczegółowymi w tym zakresie.

8.3 Uprawniony personel podmiotu nadzorowanego dokonuje przeglądu logów zgodnie z udokumentowanymi procedurami i zasadami bezpieczeństwa, przy czym – zależnie od skali działania, rodzaju i liczby logowanych zdarzeń oraz architektury bezpieczeństwa – Nadzór zaleca używanie specjalistycznego oprogramowania do korelowania zapisów ze zdarzeń (SIEM) oraz regularny przegląd i aktualizację reguł korelacji.

OPIS WYMAGAŃ

5.16.1. W zakresie monitorowania środowiska przetwarzania informacji w Usłudze chmury obliczeniowej Podmiot nadzorowany powinien:

1) posiadać udokumentowane zasady zbierania logów związanych z przetwarzaniem informacji w Chmurze obliczeniowej, stosownie do zakresu używanych Usług chmury obliczeniowej, przetwarzanych informacji i wyników szacowania ryzyka;
2) zabezpieczać logi przed nieautoryzowanym dostępem, modyfikacją lub usunięciem przez okres zgodny z ustalonymi zasadami bezpieczeństwa wynikającymi z szacowania ryzyka oraz obowiązującymi przepisami szczegółowymi w tym zakresie;
3) w zależności od skali działania, ilości logów etc. rozważyć przekazywanie logów z Chmury obliczeniowej do systemu SIEM oraz opracowanie reguł korelacji pozwalających na wykrycie incydentu bezpieczeństwa w Chmurze obliczeniowej.

5.16.2. Monitorowanie może odbywać się na różnych poziomach stosu technologicznego, przy czym istotne jest spojrzenie na ten aspekt w dwóch perspektywach – platformowej oraz aplikacyjnej, które mogą różnić się zakresem odpowiedzialności realizowanych działań przez zaangażowane podmioty (Podmiot nadzorowany, Dostawca usług chmury obliczeniowej, poddostawca chmury obliczeniowej) oraz zakresem informacji logowanych przez narzędzia do monitorowania. Ze względu na fakt, iż logi mogą również zawierać informacje będące Tajemnicą zawodową, w ramach analizy wymagań związanych z systemem monitorowania pomocne może być uwzględnienie pytań zawartych w Załączniku nr 20 „Monitorowanie”.

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.16.3. Udokumentowane zasady zbierania logów związanych z przetwarzaniem informacji w chmurze obliczeniowej.

5.16.4. Udokumentowana procedura zabezpieczania logów dla danej usługi.

5.16.5. Udokumentowane potwierdzenie dokonania przeglądu logów w ramach danej usługi.

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.16.6. Dokumentacja w zakresie logowania zdarzeń w Chmurze obliczeniowej, a także możliwości integracji mechanizmów logowania w chmurze z systemem SIEM wykorzystywanym przez Podmiot nadzorowany.

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.16.7. **Załącznik nr 20** – Monitorowanie.

5.17. DOSTĘP ADMINISTRACYJNY

8.4 **[Dostęp administracyjny]** Wymagania w stosunku do podmiotu nadzorowanego w zakresie zarządzania dostawcami usług mającymi dostęp zdalny do usług chmury obliczeniowej wykorzystywanych przez podmiot nadzorowany:

a) podmiot nadzorowany zapewnia, że wyłącznie uprawniony personel dostawcy usług ma dostęp do wskazanych systemów teleinformatycznych lub ich wybranych zakresów;

b) podmiot nadzorowany wymaga używania przez personel dostawcy usług uwierzytelnienia MFA, przy czym rodzaj i zakres uzależniony jest od wyników szacowania ryzyka;

c) podmiot nadzorowany zapewnia, że dostęp administracyjny lub o charakterze uprzywilejowanym realizowany jest z zaufanych sieci podmiotu nadzorowanego lub dostawcy usług i pod kontrolą (w tym np. poprzez nagrywanie sesji i jej parametrów, a następnie poprzez analizowanie prawidłowości i celowości realizowanych czynności), chyba że z szacowania ryzyka wynika uzasadniony brak takiej potrzeby.

OPIS WYMAGAŃ

5.17.1. Wymagania te dotyczą sytuacji, w której Podmiot nadzorowany zleca swojemu dostawcy usług wykonanie działań na zasobach podmiotu nadzorowanego umieszczonych w chmurze obliczeniowej (np. aktualizacja oprogramowania, prace serwisowe). Chodzi tu o innego dostawcę niż dostawca usługi chmury obliczeniowej, np. w sytuacji skorzystania z outsourcingu funkcji IT obejmującego zarządzanie zasobami w chmurze obliczeniowej podmiotu nadzorowanego.

5.17.2. Dostęp personelu dostawcy usług do systemów wykorzystywanych w Chmurze obliczeniowej powinien być zabezpieczony przez silne, wieloskładnikowe uwierzytelnienie.

5.17.3. Personel dostawcy powinien uzyskiwać dostęp wyłącznie z bezpiecznych stacji roboczych/terminali, zlokalizowanych w bezpiecznej (zaufanej) lokalizacji sieciowej.

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.17.4. Udokumentowane procedury lub zapisy umowne potwierdzające ograniczenie dostępu wyłącznie do uprawnionego personelu dostawcy z bezpiecznych lokalizacji sieciowych i stacji roboczych/terminali.

5.17.5. Opis mechanizmów uwierzytelnienia.

5.17.6. Udokumentowane procedury okresowej weryfikacji dostępu dostawcy do systemów wykorzystywanych w usłudze.

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.17.7. Używanie przez personel dostawcy, mający dostęp zdalny do środowiska chmury obliczeniowej Podmiotu nadzorowanego, uwierzytelnienia MFA oraz bezpiecznych stacji w bezpiecznych lokalizacjach sieciowych.

5.17.8. W zależności od wyników analizy ryzyka przeprowadzanej przez Podmiot nadzorowany, określenie innych mechanizmów zapewniających monitorowanie dostępu i rozliczalność działań dostawcy, np. nagrywanie sesji i jej parametrów w przypadku dostępu administracyjnego Dostawcy lub dostępu personelu Podmiotu nadzorowanego o charakterze uprzywilejowanym.

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.17.9. Brak.

5.18. DOKUMENTOWANIE DZIAŁAŃ PODMIOTU NADZOROWANEGO

9.1 Tam, gdzie jest to zasadne, zależnie od zakresu i rodzaju przetwarzanych informacji, zasad i regulacji obowiązujących i przyjętych w organizacji (z uwzględnieniem powiązań korporacyjnych i grupowych, jeżeli występują) oraz wyników szacowania ryzyka i przy uwzględnieniu zasady proporcjonalności, podmiot nadzorowany posiada dokumentację zawierającą:

a) organizację pracowników lub współpracowników odpowiedzialnych za cyberbezpieczeństwo, w tym stanowisk lub funkcji związanych z monitorowaniem, analizowaniem i raportowaniem incydentów związanych z informacjami przetwarzanymi w chmurze obliczeniowej, wraz z opisanymi wymaganymi kompetencjami, uprawnieniami i odpowiedzialnościami;

b) architekturę sieci, systemów i aplikacji oraz punktów styku sieci wewnętrznych podmiotu nadzorowanego z sieciami niezaufanymi, w tym architekturę rozwiązania w chmurze obliczeniowej, także z uwzględnieniem środowisk testowych oraz scenariuszy awaryjnych;

c) zasady kategoryzacji informacji lub systemów pod kątem przetwarzania w chmurze obliczeniowej lub odniesienie do obecnie funkcjonujących klasyfikacji, jeżeli mogą być stosowane;

d) zasady stosowanych zabezpieczeń technologicznych i rozwiązań organizacyjnych;

e) zasady zarządzania ciągłością działania;

f) zasady bieżącego zabezpieczania przetwarzanych informacji oraz w sytuacji planowanego lub nieplanowanego zakończenia współpracy z dostawcą usług chmury obliczeniowej;

g) zasady zarządzania zgodnością z prawem (m.in. procesy licencjonowania oprogramowania), w tym zgodnością z wymogami regulacyjnymi;

h) zasady przeglądu i weryfikacji zarządczej systemu bezpieczeństwa związanego z używaniem usług chmury obliczeniowej;

i) zasady raportowania, przeglądania i weryfikowania parametrów jakościowych funkcjonowania usług chmury obliczeniowej;

j) umowy z dostawcami usług chmury obliczeniowej wraz z dodatkowymi oświadczeniami, jeżeli to konieczne dla potwierdzenia spełnienia wymagań;

k) procesy, procedury lub instrukcje dotyczące:

   i. analizy zagrożeń i szacowania ryzyka, w tym źródła pozyskiwania informacji o zagrożeniach specyficznych dla stosowanych usług chmury obliczeniowej oraz sektora finansowego;

ii. zarządzania środowiskiem teleinformatycznym (sieciami, systemami, aplikacjami, bazami danych, itp.), z uwzględnieniem usług chmury obliczeniowej, w tym planowanie, rozwój i utrzymywanie;

iii. zarządzania logami;

iv. zarządzania kluczami szyfrującymi;

v. zarządzania incydentami bezpieczeństwa;

vi. przeprowadzania audytów wewnętrznych bezpieczeństwa teleinformatycznego z uwzględnieniem specyfiki chmury obliczeniowej.

9.2 Dokumentacja jest chroniona przed nieuprawnionym dostępem, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem. Zasady zarządzania dokumentacją podmiot nadzorowany definiuje w ramach systemu zarządzania organizacją.

OPIS WYMAGAŃ

5.18.1. Rozdział VII pkt 9 Komunikatu określa wymogi organizacyjne i dokumentacyjne, które Podmiot nadzorowany powinien posiadać (np. w charakterze polityk lub innych regulacji) chcąc wdrażać Usługi chmury obliczeniowej.

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.18.2. Udokumentowanie organizacji pracowników lub współpracowników Podmiotu nadzorowanego odpowiedzialnych za cyberbezpieczeństwo, z uwzględnieniem elementów z pkt 9 a) fragmentu Komunikatu cytowanego powyżej.

5.18.3. Udokumentowanie architektury sieci, systemów i aplikacji oraz punktów styku sieci wewnętrznych Podmiotu nadzorowanego z sieciami niezaufanymi, w tym architektury wdrażanego rozwiązania w Chmurze obliczeniowej z uwzględnieniem środowisk testowych oraz scenariuszy awaryjnych.

5.18.4. Udokumentowanie zasad kategoryzacji informacji lub systemów pod kątem przetwarzania w Chmurze.

5.18.5. Udokumentowane zasady (polityka) stosowanych w organizacji zabezpieczeń technologicznych i rozwiązań organizacyjnych w odniesieniu do rozwiązań w Chmurze obliczeniowej.

5.18.6. Udokumentowane zasady bieżącego zabezpieczania przetwarzanych informacji oraz w sytuacji planowanego lub nieplanowanego zakończenia współpracy z Dostawcą usług chmury obliczeniowej.

5.18.7. Udokumentowane zasady (polityka) zarządzania ciągłością działania.

5.18.8. Dla wdrażanej Usługi chmury obliczeniowej, udokumentowane zasady bieżącego zabezpieczania przetwarzanych informacji, jak również dla sytuacji planowanego lub nieplanowanego zakończenia współpracy z Dostawcą.

5.18.9. Udokumentowane zasady (polityka) zarządzania zgodnością z prawem (m.in. procesy licencjonowania oprogramowania), w tym zgodnością z wymogami regulacyjnymi.

5.18.10. Udokumentowane zasady (polityka) przeglądu i weryfikacji zarządczej systemu bezpieczeństwa związanego z używaniem Chmury obliczeniowej (np. coroczny przegląd).

5.18.11. Udokumentowane zasady (polityka) raportowania, przeglądania i weryfikowania parametrów jakościowych funkcjonowania Usług chmury obliczeniowej.

5.18.12. Umowa z Dostawcą wraz z dodatkowymi oświadczeniami, jeżeli to konieczne dla potwierdzenia spełnienia wymagań.

5.18.13. Udokumentowane zasady analizy zagrożeń i szacowania ryzyka dla stosowanych usług chmury obliczeniowej.

5.18.14. Udokumentowane zasady zarządzania środowiskiem teleinformatycznym, z uwzględnieniem usług chmury obliczeniowej.

5.18.15. Udokumentowane zasady zarządzania incydentami bezpieczeństwa.

5.18.16. Udokumentowane zasady przeprowadzania audytów wewnętrznych bezpieczeństwa teleinformatycznego z uwzględnieniem specyfiki chmury obliczeniowej.

5.18.17. Udokumentowane zasady zarządzania politykami i dokumentacją w ramach systemu zarządzania organizacją, zapewniające ochronę przed nieuprawnionym dostępem, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem.

ZADANIA / PRODUKTY PO STRONIE DOSTAWCY

5.18.18. Udokumentowanie architektury rozwiązania w Chmurze obliczeniowej, z uwzględnieniem środowisk testowych oraz scenariuszy awaryjnych.

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.18.19. **Załącznik nr 1** – Lista produktów do opracowania po stronie Podmiotu nadzorowanego.

5.18.20. **Załącznik nr 8** – Ankieta dla dostawców usługi chmurowej.

5.18.21. **Załącznik nr 9** – Ankieta dla dostawców – udokumentowanie konfiguracji usługi.

5.19. ZASADY INFORMOWANIA UKNF O ZAMIARZE PRZETWARZANIA LUB PRZETWARZANIU INFORMACJI W CHMURZE OBLICZENIOWEJ

VIII. ZASADY INFORMOWANIA UKNF O ZAMIARZE PRZETWARZANIA LUB PRZETWARZANIU INFORMACJI W CHMURZE OBLICZENIOWEJ

1. W przypadkach outsourcingu szczególnego chmury obliczeniowej lub przetwarzania informacji prawnie chronionej podmiot nadzorowany w terminie 14 dni przed rozpoczęciem przetwarzania informacji w chmurze obliczeniowej (a w przypadku, gdy przetwarzanie to już jest realizowane – nie później niż 1 sierpnia 2020 r.) informuje UKNF o:
   1) rodzaju i zakresie informacji planowanych do przetwarzania / przetwarzanych w chmurze obliczeniowej;
   2) nazwie dostawcy usług chmury obliczeniowej oraz rodzaju planowanych do używania / używanych usług chmury obliczeniowej;
   3) dacie podpisania umowy z dostawcą usług chmury obliczeniowej oraz terminach jej obowiązywania, a w przypadku, gdy umowa nie jest jeszcze zawarta – przewidywaną datę jej zawarcia;
   4) lokalizacji (kraj, region albo inne równoważne) centrum przetwarzania danych (CPD) świadczącym usługę chmury obliczeniowej;
   5) spełnieniu wymagań opisanych w niniejszym komunikacie;
   6) osobach lub stanowiskach do kontaktu w sprawie stosowania chmury obliczeniowej w podmiocie nadzorowanym.
2. Powyższa informacja powinna zostać podpisana przez uprawnionego przedstawiciela podmiotu nadzorowanego oraz dostarczona do UKNF przy wykorzystaniu formularza stanowiącego załącznik nr 1 do niniejszego komunikatu.

OPIS WYMAGAŃ

5.19.1. Komunikat wymaga poinformowania UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w Chmurze obliczeniowej wyłącznie w dwóch przypadkach:

1) usługi Chmury obliczeniowej stanowią Outsourcing szczególny lub
2) w ramach Outsourcingu w Chmurze obliczeniowej przetwarzana jest Tajemnica zawodowa.

5.19.2. Zgłoszenia należy dokonać 14 dni przed rozpoczęciem przetwarzania informacji w Chmurze obliczeniowej, co oznacza, że znaczenia nie ma samo zawarcie umowy outsourcingowej, ale przekazanie danych (informacji) do Dostawcy, w tym objętych Tajemnicą zawodową (bez względu na to czy w fazie przedprodukcyjnej, czy już w fazie produkcyjnej – w tym w odniesieniu np. do środowisk pre-prod.

5.19.3. Uprawnionym do podpisania informacji, o której mowa w rozdziale VIII Komunikatu jest zarówno zarząd Podmiotu nadzorowanego (zgodnie z reprezentacją w KRS), jak i osoby właściwie przez zarząd umocowane. Decyzja może mieć formę uchwały zarządu.

5.19.4. W Załączniku nr 21 do Modelu znajduje się przykład notyfikacji wymaganej Komunikatem wraz z komentarzami.

5.19.5. Przepisy UFI przewidują niezależny i dalej idący tryb powiadamiania UKNF o outsourcingu. Zgodnie z art. 45a. ust. 3. UFI Podmiot nadzorowany niezwłocznie informuje UKNF o zamiarze zawarcia umowy Outsourcingu regulowanego, a także o zamiarze zmiany umowy w odniesieniu do zakresu powierzenia wykonywanych czynności, a następnie przekazuje UKNF informacje o jej zawarciu, zmianie jej zakresu i rozwiązaniu. Dodatkowo, Podmiot nadzorowany uprzednio powiadamia UKNF o zamiarze powierzenia przez Dostawcę wykonywania czynności poddostawcom.

ZADANIA / PRODUKTY PO STRONIE PODMIOTU NADZOROWANEGO

5.19.6. Wypełniony i podpisany przez odpowiednio umocowane osoby Załącznik 1 do Komunikatu.

WYMAGANIA DO ZAADRESOWANIA/PRODUKTYDO OPRACOWANIA PO STRONIE DOSTAWCY

5.19.7. Brak.

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

5.19.8. **Załącznik 21** – Przykład notyfikacji do UKNF.

6. OUTSOURCING REGULOWANY

KOMENTARZ DO PRZEPISÓW OUTSOURCINGU REGULOWANEGO UFI

6.1.1. Kwalifikacja Usługi chmury obliczeniowej jako usługi wymagającej stosowania Komunikatu jest odrębnym zagadnieniem od kwalifikacji jako Outsourcing regulowany, o którym mowa w art. 45a ust. 1 (outsourcing TFI) lub art. 70g ust. 1 (outsourcing ASI) UFI, co należy każdorazowo zweryfikować.

6.1.2. W przypadku gdy Outsourcing chmury obliczeniowej stanowi Outsourcing Regulowany, należy zweryfikować, czy będzie to Umowa Nieistotna (zgodnie z definicją). Sytuacja taka w szczególności może mieć miejsce, jeżeli dla usługi Komunikat znajduje zastosowanie wyłącznie na podstawie spełnienia przesłanki dotyczącej przetwarzania Informacji prawnie chronionych, nie zachodzi natomiast Outsourcing szczególny chmury obliczeniowej. W takiej sytuacji, do Umowy Nieistotnej zastosowanie znajduje ograniczony zestaw wymogów określonych w art. 45a. UFI:

1) umowa zawarta w formie pisemnej (zagadnienie omówione w pkt. 5.5 Modelu), zawarta z przedsiębiorcą lub przedsiębiorcą zagranicznym (art. 45a ust.1 UFI);
2) powierzenie wykonywania czynności nie może prowadzić do zaprzestania faktycznego wykonywania działalności, o której mowa w art. 45 UFI przez Podmiot nadzorowany;
3) Podmiot nadzorowany jest obowiązany do bieżącego nadzorowania wykonywania powierzonych czynności, bez względu na podmiot je wykonujący (art. 45a ust. 4a UFI);
4) wymóg dotyczący umowy - w przypadku przekazania lub dalszego przekazania wykonywania czynności związanych z działalnością prowadzoną przez Podmiot nadzorowany przedsiębiorca lub przedsiębiorca zagraniczny jest obowiązany do bieżącego nadzorowania ich wykonywania przez podmiot, któremu przekazał ich wykonywanie (art. 45a ust. 4d. UFI);
5) zawarcie umowy nie zwalnia Podmiotu nadzorowanego z odpowiedzialności, o której mowa w art. 64 ust. 1. UFI (art. 45a ust. 5. UFI).

6.1.3. Jeżeli Outsourcing chmury obliczeniowej będzie stanowił Outsourcing regulowany, a do tego nie będzie stanowił Umowy Nieistotnej, zastosowanie znajdzie pełen zestaw wymogów:

1) Wymogi minimalne określone w pkt. 6.1.2 Modelu;
2) Wymogi w zakresie notyfikowania UKNF o zawarciu i zmianach umowy, omówione w pkt 5.19. Modelu;
3) Wymogi wobec treści umowy omówione w pkt 5.5. Modelu;

4) Powierzenie wykonywania czynności nie wpłynie niekorzystnie na sprawowanie przez Komisję efektywnego nadzoru nad towarzystwem (art. 45a ust. 4. pkt 1) UFI);

5) Podmiot nadzorowany jest w stanie obiektywnie uzasadnić powierzenie wykonywania danej czynności oraz zakres tego powierzenia, a także wykazać zachowanie należytej staranności w wyborze przedsiębiorcy lub przedsiębiorcy zagranicznego, któremu powierzane jest wykonywanie czynności; (art. 45a ust. 4. pkt 1a) UFI);

6) Powierzenie wykonywania czynności nie wpłynie niekorzystnie na prowadzenie przez Podmiot nadzorowany działalności zgodnie z interesem uczestników funduszu inwestycyjnego (art. 45a ust. 4. pkt 2) UFI);

7) Dodatkowe wymogi w zakresie podoutsourcingu, opisane szerzej w pkt. 6.1.4 Modelu;

8) Odpowiedzialność solidarna określona w art. 45a ust. 6 UFI, zgodnie z którym Podmiot nadzorowany odpowiada za szkody wywołane niewykonaniem lub nienależytym wykonaniem umowy wobec uczestników funduszu solidarnie z Dostawcą oraz poddostawcami Dostawcy, chyba że szkoda ta wynika z okoliczności, za które podmioty te nie ponoszą odpowiedzialności.

6.1.4. Podoutsourcing.

1) Zarówno podoutsourcing, jak i podoutsourcing łańcuchowy są zasadniczo dopuszczalne w ramach Outsourcingu regulowanego.

2) Jeśli Usługa chmury obliczeniowej jest jednocześnie Outsourcingiem regulowanym w rozumieniu art. 45a ust. 1 lub art. 70g ust.1 UFI, to podmiotem któremu przedsiębiorca lub przedsiębiorca zagraniczny powierza lub dalej powierza wykonywanie czynności w odniesieniu do takiej Usługi jest w szczególności podmiot, który spełnia wymogi definicji „poddostawcy" z Komunikatu.

3) W przypadku Outsourcingu chmury obliczeniowej, który kwalifikuje się jako Outsourcing regulowany, a jednocześnie kwalifikuje się jako Umowa Nieistotna, postanowienia umowy powinny zapewniać pełną odpowiedzialność Dostawcy za działania i zaniechania podmiotów, którym dalej powierza wykonywanie czynności. Dotyczy to w szczególności „poddostawców" - zgodnie z definicją.

4) W przypadku Outsourcingu chmury obliczeniowej, który kwalifikuje się jako Outsourcing regulowany, a jednocześnie nie kwalifikuje się jako Umowa Nieistotna, zastosowanie znajdują dodatkowe wymogi opisane w art. 45a ust. 4c. UFI, na podstawie którego odpowiednio stosuje się art. 45a ust. 4b UFI. W takiej sytuacji Dostawca może przekazać wykonywanie powierzonych mu czynności innemu przedsiębiorcy lub przedsiębiorcy zagranicznemu wyłącznie:

   a) za zgodą Podmiotu nadzorowanego i po uprzednim poinformowaniu przez Podmiot nadzorowany Komisji o zamiarze takiego przekazania na zasadach przewidzianych dla powiadomienia o zmianie (opisanych w art. 45a ust. 3 UFI) oraz

   b) jeżeli w odniesieniu do przedsiębiorcy lub przedsiębiorcy zagranicznego, któremu ma być przekazane wykonywanie czynności, spełnione są warunki określone w art. 45a ust. 4 UFI, tj. analogiczne wymogi przewidziane dla umowy oraz dla Podmiotu nadzorowanego.

6.1.5. Zastrzeżenie z art. 47 ust.6 UFI, zgodnie z którym do Outsourcingu regulowanego „wykonywania czynności związanych z prowadzoną przez towarzystwo działalnością w zakresie zarządzania portfelami, w skład których wchodzi jeden lub większa liczba instrumentów finansowych, doradztwa inwestycyjnego oraz przyjmowania i przekazywania zleceń nabycia lub zbycia instrumentów finansowych stosuje się odpowiednio przepisy art. 81a ust. 1 i 2, art. 81c, art. 81d oraz art. 81f ustawy o obrocie instrumentami finansowymi.” dotyczy przede wszystkim outsourcingu czynności wymienionych w tym przepisie, obejmujących zasadniczo czynności doradztwa inwestycyjnego (outsourcing czynności maklerskich). O ile Outsourcing chmury obliczeniowej nie jest funkcjonalnie powiązany z outsourcingiem w/w czynności, do takiego Outsourcingu regulowanego nie stosujemy w/w przepisów Ustawy o obrocie.

6.1.6. Outsourcing regulowany zlecany przez Podmioty nadzorowane stanowiące ASI jest uregulowany w art. 70g UFI, który zawiera regulacje zasadniczo albo analogiczne do art. 45a UFI albo przewidujące odpowiednie stosowanie tego ostatniego przepisu, z wyłączeniem art. 45a ust. 8 UFI opisującego przykładowe Umowy Nieistotne. W tym zakresie można jednak polegać na ogólnej zasadzie prawnej stosowania tego przepisu *per analogiam*.

7. ZAŁĄCZNIKI

Załącznik 1. Lista produktów do opracowania po stronie Podmiotu nadzorowanego	
Załącznik 2. Klasyfikacja informacji - skoroszyt	
Załącznik 3. Klasyfikacja informacji – opis zagadnień	
Załącznik 4. Szablon szacowania ryzyka	
Załącznik 5. Lista przykładowych zagrożeń i podatności	
Załącznik 6. Kwestionariusz - okresowe monitorowanie umów	
Załącznik 7. Wymagania dla dostawców usług chmurowych zgodnie z Komunikatem	
Załącznik 8. Ankieta dla dostawców usługi chmurowej	
Załącznik 9. Ankieta dla dostawców – udokumentowanie konfiguracji usługi	

Załącznik 10. Fazy projektu wdrożenia usługi chmurowej – materiał pomocniczy	
Załącznik 11. Nadzór (governance)	
Załącznik 12. Wybrane definicje i pojęcia związane z bezpieczeństwem informacji	
Załącznik 13. Objaśnienia i lista wybranych klauzul wraz z przykładami	
Załącznik 14. Plan przetwarzania informacji w chmurze obliczeniowej	
Załącznik 15. Szablon scenariusza wyjścia z relacji z Dostawcą	
Załącznik 16. Wyjście z chmury – główne zagadnienia	
Załącznik 17. Szablon dokumentacji kontroli ISO27001	
Załącznik 18. Lista zagadnień dla wyboru dostawców związanych z bezpieczeństwem	
Załącznik 19. Kryptografia	
Załącznik 20. Monitorowanie	
Załącznik 21. Przykład notyfikacji do UKNF	