Standard wdrożeń przetwarzania informacji w chmurze obliczeniowej

w branży zarządzania wierzytelnościami

Związek Przedsiębiorstw Finansowych w Polsce

We współpracy z:

RYMARZ ZDORT MARUTA

TKP Traple Konarski Podrecki & Wspólnicy

Związek Przedsiębiorstw Finansowych w Polsce

Związek Przedsiębiorstw Finansowych w Polsce (wcześniej Konferencja Przedsiębiorstw Finansowych w Polsce – Związek Pracodawców) powstał 27 października 1999 roku i obecnie skupia około stu kluczowych przedsiębiorstw z wielu sektorów polskiego rynku finansowego, w tym bankowości, zarządzania wierzytelnościami, pośredników finansowych, instytucji pożyczkowych, zarządzających informacją gospodarczą i kredytową, odwróconej hipoteki w modelu sprzedażowym, platform crowdfundingowych oraz ubezpieczeń. ZPF to Członek Rady Rozwoju Rynku Finansowego, powołanej do życia przez Ministra Finansów Rzeczypospolitej Polskiej oraz Członek prestiżowej organizacji samorządowej europejskiego przemysłu kredytowego EUROFINAS (European Federation of Finance House Associations), zrzeszającej szesnaście krajowych organizacji, reprezentujących instytucje finansowe. ZPF ma w swoim dorobku badawczym już kilkaset raportów, koncentrując się merytorycznie na obszarze kredytu.

member of eurofinas

Materiał powstał w ramach prac Zespołu ZPF ds. chmury obliczeniowej

we współpracy z:
adw. Michał Kulesza, Rymarz, Zdort, Maruta, Wachta, Gasiński, Her i Wspólnicy sp.k.
Aleksandra Grześkowiak, Rymarz, Zdort, Maruta, Wachta, Gasiński, Her i Wspólnicy sp.k.
adw. Jan Byrski, Traple Konarski Podrecki i Wspólnicy Sp.j.
adw. Michał Synowiec, Traple Konarski Podrecki i Wspólnicy Sp.j.

Warszawa, czerwiec 2023

Związek Przedsiębiorstw Finansowych w Polsce
ul. Długie Pobrzeże 30
80-888 Gdańsk
info@zpf.pl

Spis treści

I. WSTĘP

1. Założenia i adresaci Standardu

Implementacja technologii chmury obliczeniowej to wymagający projekt prawny i technologiczny oraz potężne wyzwanie organizacyjne. Ze względu na podwyższone standardy bezpieczeństwa i wymogi regulacyjne, odczuwać może to w szczególności sektor finansowy. Wydany w styczniu 2020 r. Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej wspiera proces wdrożenia technologii chmurowych poprzez zaadaptowanie wymagań regulacyjnych do specyfiki technologicznej. Jednocześnie zasady wynikające z przepisów outsourcingowych i złożone powiązania między poszczególnymi podmiotami rynku finansowego otwierają kolejny poziom zniuansowanych wymogów, specyficznych dla poszczególnych sektorów.

Dlatego też, mając na względzie aprobatę UKNF dla inicjatyw standaryzacji wdrożenia rozwiązań chmurowych podejmowanych przez zrzeszenia sektora finansowego, Związek Przedsiębiorstw Finansowych w Polsce jako organizacja zrzeszająca około stu przedsiębiorstw z rynku finansowego, zdecydował się na zaadresowanie wyzwań, przed którymi w procesie wdrożenia usługi chmurowej stoją podmioty z branży zarządzania wierzytelnościami, a w szczególności podmioty posiadające zezwolenie KNF na zarządzanie sekurytyzowanymi wierzytelnościami funduszu sekurytyzacyjnego. Prowadząc działalność gospodarczą, takie przedsiębiorstwa, co najmniej w zakresie w jakim podlegają nadzorowi UKNF, powinny uwzględniać odpowiednie przepisy prawa oraz wytyczne nadzoru finansowego.

Wątpliwości praktyczne zidentyfikowane w ramach prac nad Standardem zostały zaadresowane poprzez skierowanie do UKNF dodatkowych pytań dotyczących wybranych aspektów stosowania Komunikatu chmurowego UKNF. Zadane pytania wraz z odpowiedziami zawarto w Załączniku nr 10 do Standardu.

Bezpośrednie stosowanie Komunikatu chmurowego UKNF

W przypadku, w którym Zarządzający wierzytelnościami, posiadający zezwolenie na zarządzanie sekurytyzowanymi wierzytelnościami funduszu sekurytyzacyjnego zdecyduje się na implementację rozwiązania opartego o chmurę publiczną lub hybrydową, w związku z działaniami realizowanymi w oparciu o zezwolenie, o którym mowa wyżej, i w ramach procesu chmurowego zachodzi przetwarzanie Informacji prawnie chronionych lub outsourcing szczególny chmury obliczeniowej – to taki zarządzający powinien liczyć się z potrzebą respektowania wymogów Komunikatu chmurowego UKNF. Natomiast inne podmioty profesjonalnie zajmujące się zarządzaniem wierzytelnościami z formalnego punktu widzenia Komunikat chmurowy UKNF „bezpośrednio" stosują w sposób dobrowolny. Uwzględnienie wytycznych UKNF pozwala takim przedsiębiorcom na dorównanie poziomem bezpieczeństwa wykorzystywanej technologii do standardów przyjętych przez podmioty nadzorowane sektora finansowego. Wszyscy przedsiębiorcy z branży zarządzających

wierzytelnościami Komunikat chmurowy UKNF powinni postrzegać zatem jako dokument, który najlepiej na rynku „rozumie" technologie chmurowe i stanowi odpowiedni przewodnik po ich implementacji w organizacji.

Wsparcie nadzorowanych Partnerów biznesowych w weryfikacji spełnienia wymogów regulacyjnych i nadzorczych

Druga kategoria stojących przed Zarządzającymi wierzytelnościami wyzwań o charakterze regulacyjnym wynika ze współpracy z innymi podmiotami z sektora nadzorowanego. Zarządzający wierzytelnościami, aby utrzymać ciągłość relacji biznesowych w związku z przeprowadzaną transformacją cyfrową, powinni liczyć się z potrzebą uwzględnienia oczekiwań swoich Partnerów biznesowych. Mianowicie Podmioty nadzorowane takie jak TFI, Zakłady Ubezpieczeń i Banki, decydując się na powierzenie wykonywania czynności Zarządzającym wierzytelnościami, którzy wykorzystują chmurę obliczeniową do świadczenia usług, są zmuszeni zadbać o zapewnienie zgodności dokonanego powierzenia z przepisami prawa i wymogami nadzoru w ramach całego łańcucha outsourcingowego.

Warto zatem, aby również Zarządzający nieposiadający licencji, na możliwie najwcześniejszym etapie implementacji chmury obliczeniowej w przedsiębiorstwie, wzięli pod uwagę zasadę *compliance-by-design*. Zasada ta wiąże się z potrzebą zaprojektowania wdrożenia chmurowego nie tylko z uwzględnieniem wymogów bezpośrednio ciążących na Zarządzających nieposiadających licencji, ale także tych, które mogą ich dotknąć pośrednio – z uwagi na potrzebę wsparcia powierzających im czynności Podmiotów nadzorowanych. Takie Podmioty nadzorowane powinny zapewnić, że przetwarzanie informacji w łańcuchu outsourcingowym jest realizowane z uwzględnieniem wymogów przepisów prawa i Komunikatu chmurowego UKNF. Stąd też dla utrzymania relacji biznesowych Zarządzający nieposiadający licencji, planujący wykorzystywać chmurę obliczeniową na potrzeby wykonywania przekazywanych im czynności, powinni liczyć się z koniecznością nie tylko uwzględnienia wymogów Komunikatu chmurowego UKNF, ale również „przeniesienia" wymogów outsourcingowych wiążących Partnerów biznesowych z sektora nadzorowanego na umowy wiążące Zarządzających nieposiadających licencji z dostawcami usług chmurowych oraz na samą metodykę wdrożenia.

2. Zakres Standardu

Korzystanie z rozwiązań chmurowych bez wątpienia przynosi organizacjom duże korzyści i zmienia model ich funkcjonowania. Dzięki nim podmioty z sektora finansowego mogą sprawniej reagować na zmieniającą się sytuację rynkową oraz potrzeby klientów, ograniczając przy tym koszty infrastruktury IT. Ze względu na związane z migracją chmurową wyzwania i potrzebę pogodzenia wielu racji, Związek Przedsiębiorstw Finansowych przy aktywnym udziale zrzeszonych przedsiębiorstw zarządzających wierzytelnościami oraz kancelarii prawnych Rymarz Zdort Maruta oraz Traple Konarski Podrecki i Wspólnicy, postanowił opracować **Standard wdrożeń przetwarzania informacji w chmurze obliczeniowej w branży zarządzania wierzytelnościami.**

Dokument **standaryzuje podejście branży Zarządzających wierzytelnościami względem wytycznych Komunikatu chmurowego UKNF w korelacji z właściwymi dla tych podmiotów przepisami sektorowymi**. Standard może być wykorzystany jako przykładowy model postępowania przez podmioty Zarządzające wierzytelnościami w projektach chmurowych, niemniej każdorazowo jego stosowanie powinno możliwie najszerzej uwzględniać specyfikę działalności danego Podmiotu nadzorowanego. Standard ma stanowić praktyczny przewodnik po klasyfikacji i ocenie informacji, procesie szacowania ryzyka oraz kompletowania niezbędnej z punktu widzenia Komunikatu chmurowego UKNF dokumentacji. Dokument, mając na celu najlepsze przygotowanie firm Zarządzających wierzytelnościami do implementacji rozwiązań chmurowych, uwzględnia również specyfikę typowych dla chmury ryzyk i momentów krytycznych migracji – wynikających z relacji z dostawcą technologii, zagrożeń dla ciągłości działania czy szyfrowania danych i lokalizacji serwerów.

Ponadto **Standard punktowo porusza wyzwania, z którymi mierzą się podmioty Zarządzające wierzytelnościami w ramach współpracy z Podmiotami nadzorowanymi z sektora finansowego**: uwzględnia działania, które Zarządzający wierzytelnościami powinni podjąć w szczególności przy zamiarze przetwarzania w chmurze obliczeniowej informacji objętych tajemnicą sektora finansowego.

Wykorzystanie dokumentu w procesie migracji chmurowej – również przez podmioty bezpośrednio do tego nie zobowiązane – pozwoli utrzymać podmiotom Zarządzającym wierzytelnościami wysokie standardy postępowania w relacjach z klientami i kontrahentami, z zachowaniem odpowiedniego poziomu bezpieczeństwa i zasad postępowania z danymi. Inicjatywa standaryzacji ma na celu ułatwienie drogi do cyfryzacji branży zarządzających wierzytelnościami, tak aby rozwiązania chmurowe mogły stać się trwałą częścią ich strategii biznesowych.

Stąd też przedstawione w niniejszym Standardzie zalecenia dla Zarządzających posiadających licencję, którzy zobowiązani są do Bezpośredniego stosowania Komunikatu chmurowego UKNF zgodnie z określonymi w Komunikacie przesłankami mogą być odpowiednio stosowane przez Zarządzających nieposiadających licencji w przypadku podjęcia takiej decyzji wewnętrznej. Zaznaczyć jednak należy, że Standard w żadnym przypadku nie stanowi zbioru wytycznych przeważających nad Komunikatem chmurowym UKNF lub innymi wymaganiami sektorowymi wymienionymi w jego treści. Komunikat chmurowy UKNF ma każdorazowo znaczenie nadrzędne nad Standardem. Objaśnienia wymogów Komunikatu chmurowego UKNF oraz praktyczne wskazówki zawarte w Standardzie nie mają na celu zastąpienia regulacji zawartej w Komunikacie chmurowym UKNF i nie powinny być interpretowane jako tworzące wymagania wykraczające poza Komunikat chmurowy UKNF.

***

Niniejszy dokument powstał w oparciu o „Standard wdrożeń przetwarzania informacji w chmurze obliczeniowej dla branży ubezpieczeniowej" Polskiej Izby Ubezpieczeń (PIU), przygotowany wspólnie przez zakłady ubezpieczeń, kancelarie Traple Konarski Podrecki i

Wspólnicy oraz Rymarz Zdort Maruta, PIIT, Accenture oraz dostawców technologii w ramach prac grupy roboczej przy PIU.

II. WYKORZYSTYWANA TERMINOLOGIA

Wykorzystane, ale niezdefiniowane w Standardzie terminy mają znaczenie nadane im w Komunikacie chmurowym UKNF.

O ile nic innego nie wynika ze Standardu, terminy wykorzystane w Standardzie należy interpretować z uwzględnieniem wytycznych Komunikatu chmurowego UKNF oraz innych wytycznych wydawanych przez KNF lub UKNF, w tym w szczególności Q&A do Komunikatu UKNF.

Poniższe terminy mają następujące znaczenie:

1. **Bank** – bank, o którym mowa w art. 4 Prawa bankowego.
2. **Bezpośrednie stosowanie Komunikatu** – stosowanie Komunikatu przez Podmioty nadzorowane zgodnie z określonymi w Komunikacie przesłankami.
3. **Dane osobowe** – dane osobowe w rozumieniu art. 4 pkt 1) Rozporządzenia 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), zwanego RODO.
4. **Dostawca** – dostawca usług chmury obliczeniowej lub inny dostawca Podmiotu nadzorowanego (np. dostawca usług IT), który korzysta z usług dostawcy usług chmury obliczeniowej, w zakresie w jakim podmiot ten wykonuje na rzecz Podmiotu nadzorowanego proces, usługę lub działanie, które w innym przypadku zostałyby wykonane przez Podmiot nadzorowany.
5. **EOG** – Europejski Obszar Gospodarczy.
6. **Informacja prawnie chroniona** – informacje objęte tajemnicami sektora finansowego, o których mowa w ustawach wskazanych w Komunikacie.
7. **KNF** – Komisja Nadzoru Finansowego.
8. **Komunikat, Komunikat chmurowy UKNF –** Komunikat UKNF z 23 stycznia 2020 r. dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej.
9. **Model usługi chmury obliczeniowej** – wariant dostarczania usługi przez dostawcę, w szczególności SaaS (*Software as a Service*), PaaS (*Platform as a Service*), IaaS (*Infrastructure as a Service*).
10. **Podmiot nadzorowany** – podmiot podlegający nadzorowi nad rynkiem finansowym zgodnie z ustawą z 21 lipca 2006 r. o nadzorze nad rynkiem finansowym, art. 1 ust. 2 pkt 1) – 8).
11. Dla uniknięcia wątpliwości w rozumieniu niniejszego Standardu za Podmiot nadzorowany uznawany jest m. in. Zarządzający posiadający licencję działający w zakresie zezwolenia KNF na zarządzanie sekurytyzowanymi wierzytelnościami uzyskanego na podstawie art. 192 UFI.
12. **Pośrednie stosowanie Komunikatu** – uwzględnienie przez Zarządzającego wymogów Komunikatu w procesie przetwarzania informacji w chmurze obliczeniowej w zakresie w jakim oczekuje tego Powierzający podmiot nadzorowany, który ma obowiązek zapewnić, że

przetwarzanie informacji w chmurze obliczeniowej przez bezpośredniego dostawcę (Zarządzającego) jest realizowane z uwzględnieniem postanowień Komunikatu.

13. **Powierzający podmiot nadzorowany, Partner** – współpracujący z Zarządzającym zobowiązany do stosowania Komunikatu Podmiot nadzorowany (w szczególności Bank, TFI), który na podstawie umowy outsourcingowej zezwala Zarządzającemu na czynność przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej (w zakresie jej części opartej o chmurę obliczeniową publiczną), w ramach której zachodzi przetwarzanie Informacji prawnie chronionych w związku z outsourcingiem chmury obliczeniowej lub outsourcing szczególny chmury obliczeniowej.
14. **Prawo bankowe** – ustawa z 29 sierpnia 1997 r. – Prawo bankowe, ze zmianami.
15. **Rozporządzenie Delegowane** - rozporządzenie delegowane Komisji (UE) 2015/35 z dnia 10 października 2014 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2009/138/WE w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II).
16. **Sekurytyzowane wierzytelności** – wierzytelności, o których mowa w art. 2 pkt. 32) UFI.
17. **Standard** – niniejszy Standard wdrożeń przetwarzania informacji w chmurze obliczeniowej w branży zarządzania wierzytelnościami.
18. **TFI, Towarzystwo** – towarzystwo funduszy inwestycyjnych spółka akcyjna.
19. **UDUR** – ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, ze zmianami.
20. **UFI** – ustawa z 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi, ze zmianami.
21. **UKNF** – Urząd Komisji Nadzoru Finansowego.
22. **Zakład Ubezpieczeń, ZU** – podmiot będący krajowym lub zagranicznym Zakładem Ubezpieczeń w rozumieniu UDUR, jak również oddziałem zagranicznego Zakładu Ubezpieczeń.
23. **Zarządzający, Zarządzający wierzytelnościami** – Zarządzający posiadający licencję oraz Zarządzający nieposiadający licencji.
24. Zarządzający m. in. wykonuje czynności powierzone przez Powierzające podmioty nadzorowane z sektora finansowego, w tym czynności związane z przetwarzaniem w chmurze obliczeniowej informacji Powierzających podmiotów nadzorowanych.
25. **Zarządzający nieposiadający licencji –** zarządzający wierzytelnościami, który nie posiada licencji na zarządzanie sekurytyzowanymi wierzytelnościami funduszu sekurytyzacyjnego uzyskanej zgodnie z art. 192 UFI.
26. **Zarządzający posiadający licencję, Serwiser** – zarządzający wierzytelnościami posiadający licencję na zarządzanie sekurytyzowanymi wierzytelnościami funduszu sekurytyzacyjnego uzyskaną zgodnie z art. 192 UFI.
27. **ZPF** – Związek Przedsiębiorstw Finansowych w Polsce.
28. **Q&A do Komunikatu UKNF** – opublikowane przez UKNF pytania i odpowiedzi (Q&A) w zakresie stosowania Komunikatu UKNF z 23 stycznia 2020 r. dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej.

III. SCHEMAT DOKUMENTU

1. Standard został podzielony na rozdziały poświęcone poszczególnym wymaganiom nadzorczym i prawnym mającym wpływ na sposób implementacji usług chmury obliczeniowej w branży Zarządzających wierzytelnościami.
2. W rozdziale IV. Standardu wskazane zostały wymogi Komunikatu wraz z opisem oraz odpowiednimi rekomendowanymi ustandaryzowanymi działaniami, jakie w ocenie autorów Standardu należy podjąć celem wdrożenia usługi chmury obliczeniowej zgodnie z danym wymogiem.
3. Podrozdziały w rozdziale IV. Standardu składają się z (w zakresie w jakim jest to zasadne):
    1) cytatu danego wymagania Komunikatu;
    2) komentarza praktycznego do wymagania;
    3) wskazania działań (produktu) po stronie Zarządzającego, w tym w zakresie Pośredniego stosowania Komunikatu;
    4) wskazania wkładu (produktu) po stronie dostawcy usług chmury obliczeniowej;
    5) odwołania do szablonów/ wzorców.
4. W rozdziale V. wskazane zostały wybrane wymogi sektorowe istotne z perspektywy podoutsourcingu chmurowego dokonywanego przez TFI i Banki, które Zarządzający, jako Dostawca Powierzającego podmiotu nadzorowanego dokonujący dalszego powierzenia czynności w związku z korzystaniem z usług dostawcy chmury obliczeniowej, powinien uwzględnić na możliwie najwcześniejszym etapie migracji chmurowej.

   Kwestie omówione w rozdziale V. mają na celu zasygnalizowanie najczęstszych wyzwań Zarządzających w związku z udziałem w łańcuchu outsourcingowym Powierzającego podmiotu nadzorowanego i koniecznością Pośredniego stosowania Komunikatu. Niemniej, uwzględnienie przez Zarządzającego wymogów Komunikatu chmurowego UKNF oraz przepisów sektorowych ciążących na Powierzającym podmiocie nadzorowanym powinno nastąpić w zakresie i w sposób określony przez taki podmiot oraz zgodnie z jego instrukcjami.

IV. KOMUNIKAT CHMUROWY UKNF

1. Wytyczne stosowania

TREŚĆ KOMUNIKATU UKNF

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 komunikacie 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

1. UKNF oczekuje stosowania Komunikatu od Podmiotów nadzorowanych. W ramach Bezpośredniego stosowania Komunikatu, Komunikat stosują zatem Zarządzający posiadający licencję w zakresie, w jakim w chmurze obliczeniowej przetwarzają informacje w związku z działaniami realizowanymi w oparciu o zezwolenie, o którym mowa w art. 192 UFI i zgodnie z przesłankami stosowania Komunikatu.
2. Zarządzający nieposiadający licencji Komunikat stosują dobrowolnie. W przypadku podjęcia decyzji wewnętrznej o stosowaniu Komunikatu przez Zarządzającego nieposiadającego licencji, podmiot taki odpowiednio uwzględnia wskazane w niniejszym Standardzie zalecenia dla Zarządzających posiadających licencję.
   - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający w przypadku przetwarzania w chmurze obliczeniowej informacji powierzonych przez Powierzające podmioty*

nadzorowane i z uwzględnieniem przesłanek stosowania Komunikatu, odpowiednio uwzględnia wymogi Komunikatu w ramach wsparcia Powierzających podmiotów nadzorowanych w wykazaniu, że przetwarzanie informacji jest realizowane z uwzględnieniem postanowień Komunikatu i przepisów prawa – zgodnie z oczekiwaniami Powierzających podmiotów nadzorowanych.

- *Zarządzający w procesie migracji chmurowej uwzględnia oczekiwania Powierzającego podmiotu nadzorowanego w szczególności w zakresie:*
  - *sposobu i ograniczeń co do korzystania z chmury obliczeniowej;*
  - *kształtu umowy Zarządzającego z dostawcą usług chmury obliczeniowej;*
  - *wkładu ze strony Zarządzającego, którego Powierzający podmiot nadzorowany oczekuje w celu weryfikacji i wykazania wypełnienia wymogów Komunikatu oraz wymagań prawnych*

- podczas działań Zarządzającego związanych z przygotowaniem, realizacją oraz zakończeniem przetwarzania informacji w chmurze obliczeniowej.

3. Komunikat ma zastosowanie w przypadku:
   1) przetwarzania Informacji prawnie chronionych w ramach outsourcingu chmury obliczeniowej (tzw. zwykłego outsourcingu), lub
   2) outsourcingu szczególnego chmury obliczeniowej.

   W każdym innym przypadku Komunikat może być stosowany, jeśli Zarządzający (również w porozumieniu z Powierzającym podmiotem nadzorowanym lub dostawcą usług chmury obliczeniowej) tak postanowi.
4. Komunikat nie odnosi się do:

   1) chmury obliczeniowej prywatnej, w tym chmury obliczeniowej społecznościowej o charakterze prywatnym;
   2) wykorzystywania usługi chmury obliczeniowej do projektowania i przetwarzania danych (informacji) testowych, które nie są Informacjami prawnie chronionymi.

5. W procesie oceny charakteru planowanego do wykorzystania rozwiązania opartego o chmurę obliczeniową w ramach dokonywania weryfikacji i kwalifikacji procesu jako podlegającego wymogom Komunikatu, Zarządzający może pomocniczo opierać się na definicji chmury obliczeniowej w rozumieniu National Institute of Standards and Technology (NIST Special Publication 800-145).
6. Przed powierzeniem przetwarzania informacji w chmurze obliczeniowej publicznej lub chmurze obliczeniowej hybrydowej (w zakresie jej części opartej o chmurę obliczeniową publiczną) Zarządzający posiadający licencję powinien:
   1) ocenić, jakie informacje są planowane do powierzenia celem zidentyfikowania, czy będą to Informacje prawnie chronione;
   2) w przypadku oceny, że nie są planowane do powierzenia informacje prawnie chronione zgodnie z pkt. 1) powyżej - wstępnie ocenić, czy powierzenie przetwarzania informacji stanowi outsourcing szczególny chmury obliczeniowej.

   Wyniki powyższej oceny powinny zostać udokumentowane, a następnie uwzględnione w procesie migracji chmurowej.

7. Wymagania określone w Komunikacie powinny być spełnione przez Zarządzającego posiadającego licencję przed rozpoczęciem przetwarzania informacji w usłudze chmury obliczeniowej.
    - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne wytyczne Powierzającego podmiotu nadzorowanego co do wstępnej klasyfikacji i oceny informacji oraz przekazuje mu wyniki przeprowadzonej weryfikacji na potrzeby wykazania przez Powierzający podmiot nadzorowany, że przetwarzanie informacji jest realizowane z uwzględnieniem postanowień Komunikatu i przepisów prawa.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO

1. Udokumentowana ocena jakie informacje są planowane do powierzenia celem zidentyfikowania, czy będą to Informacje prawnie chronione w ramach outsourcingu chmury obliczeniowej (tzw. zwykłego outsourcingu) lub wstępna ocena, czy występuje outsourcing szczególny chmury obliczeniowej.
    - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne wytyczne Powierzającego podmiotu nadzorowanego co do oczekiwanego modelu przeprowadzenia powyższych ocen i przekazuje wyniki takiej weryfikacji Powierzającemu podmiotowi nadzorowanemu.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUGI CHMURY OBLICZENIOWEJ

N/D

SZABLONY

1. **Załącznik nr 1** do Standardu – Modelowe wdrożenie usługi przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej dla Zarządzających wierzytelnościami;
2. **Załącznik nr 4** do Standardu - Założenia metodyki w zakresie przetwarzania informacji w chmurze obliczeniowej zgodnie z Komunikatem chmurowym UKNF.

2. Wytyczne do klasyfikacji i oceny informacji

TREŚĆ KOMUNIKATU UKNF

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 (lecz nie rzadziej niż raz w roku) przeglądać i potwierdzać aktualność stosowanej klasyfikacji i oceny informacji do bieżących warunków swojego działania.

OPIS WYMAGAŃ

1. Zarządzający posiadający licencję klasyfikuje i dokonuje oceny informacji w udokumentowany sposób, zgodnie z metodyką przyjętą u Zarządzającego posiadającego licencję, w tym w szczególności zapewnia, że:
   1) klasyfikacja i ocena informacji uwzględnia podział na kategorie informacji;
   2) klasyfikacja i ocena informacji uwzględnia co najmniej podział na Informacje prawnie chronione, informacje, których ochrona wynika z innych uregulowań prawnych oraz pozostałe informacje;
   3) klasyfikacja i ocena informacji uwzględnia podstawowe atrybuty bezpieczeństwa, tj. poufność, integralność i dostępność;
   4) klasyfikacja i ocena informacji uwzględnia skalę prowadzonej działalności, ewentualne wewnętrzne modele klasyfikacji i oceny informacji oraz odpowiedzialność Zarządzającego posiadającego licencję za przetwarzane informacje;
   5) proces oceny informacji uwzględnia wymogi prawa i postanowienia umów wiążących Zarządzającego posiadającego licencję, zakres przetwarzanych informacji, ich rodzaj, ważność i wartość.
      - *W ramach **Pośredniego stosowania Komunikatu,** Zarządzający uwzględnia ewentualne wytyczne Powierzającego podmiotu nadzorowanego co do klasyfikacji i oceny informacji oraz przekazuje mu wyniki przeprowadzonej weryfikacji na potrzeby wykazania przez*

Powierzający podmiot nadzorowany, że przetwarzanie informacji jest realizowane z uwzględnieniem postanowień Komunikatu i przepisów prawa.

2. Zarządzający posiadający licencję przeprowadza klasyfikację i ocenę informacji ponownie, gdy:
   1) zamierza przetwarzać nowy rodzaj informacji;
   2) zamierza wykorzystać nową usługę chmury obliczeniowej[1];
   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 (przy czym, jeżeli zasadne, Zarządzający może w ramach procedur wewnętrznych przyjąć, że w przypadku zmniejszenia skali przetwarzania informacji, ponownej klasyfikacji i oceny informacji dokonuje w przypadku, w którym dana zmiana skali przetwarzania może mieć wpływ na poziom bezpieczeństwa);
   5) istotnie zwiększa się wartość przetwarzanych informacji

   oraz na bieżąco monitoruje zmiany w zakresie wymogów prawnych oraz regulacyjnych w zakresie, który wymagałby ponownej klasyfikacji i oceny przetwarzanych informacji.

- *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne wytyczne Powierzającego podmiotu nadzorowanego co do ponownej klasyfikacji i oceny przetwarzanych informacji, a także przekazuje Powierzającemu podmiotowi nadzorowanemu informacje odnośnie wszelkich zmian w procesie chmurowym mogących wpłynąć na wyniki klasyfikacji i oceny informacji.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO

1. Udokumentowane zasady przeprowadzania klasyfikacji informacji (metodyka).
2. Udokumentowany proces klasyfikacji i oceny informacji przetwarzanych w chmurze obliczeniowej uwzględniające wytyczne opisane w rozdziale V. Komunikatu – Wytyczne do klasyfikacji i oceny informacji.
3. Udokumentowane wyniki przeprowadzonej klasyfikacji i oceny informacji, które powinny zostać uwzględnione w planie przetwarzania informacji w chmurze obliczeniowej.
4. Udokumentowane okresowe przeglądy klasyfikacji i oceny informacji (nie rzadziej niż raz w roku) wraz z potwierdzeniem aktualności stosowanej klasyfikacji i oceny informacji. Zarządzający może określić szczegółowe zasady przeprowadzania przeglądów klasyfikacji i oceny informacji w ramach procedur wewnętrznych.

---

[1] Przykładem wykorzystania nowej usługi chmury obliczeniowej może być np. (i) rozpoczęcie korzystania z określonej usługi dostawcy X, podczas gdy Zarządzający korzystał dotychczas wyłącznie z usług dostawcy Y (kryterium podmiotowe) albo (ii) nabycie od dostawcy X dodatkowej przestrzeni w chmurze obliczeniowej celem posadowienia i utrzymywania własnego rozwiązania (Rozwiązanie A) w sytuacji, w której niezależnie od Rozwiązania A Zarządzający wykorzystuje w swojej organizacji nabyty od dostawcy X pakiet aplikacji stanowiących zintegrowany zestaw narzędzi informatycznych wspierających pracę grupową (Rozwiązanie B) (kryterium przedmiotowe). Niemniej każdorazowo weryfikacja i ocena, czy nowe rozwiązanie w organizacji w ramach istniejącego procesu bądź nowy proces stanowi nową usługę chmury obliczeniowej należy do podmiotu nadzorowanego i powinna uwzględniać aspekty prawne, organizacyjne i technologiczne.

- *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne wytyczne Powierzającego podmiotu nadzorowanego co do oczekiwanego wkładu Zarządzającego w proces klasyfikacji i oceny informacji oraz przekazuje mu wyniki przeprowadzonej weryfikacji na potrzeby wykazania przez Powierzający podmiot nadzorowany, że przetwarzanie informacji jest realizowane z uwzględnieniem postanowień Komunikatu i przepisów prawa.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUGI CHMURY OBLICZENIOWEJ

N/D

SZABLONY

1. **Załącznik nr 2** do Standardu – Wzorcowa dokumentacja klasyfikacji i oceny informacji.

3. Wytyczne do szacowania ryzyka

TREŚĆ KOMUNIKATU UKNF

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 [2]. 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;

[2] Szacowanie ryzyka może być oparte o udokumentowaną i właściwie wdrożoną metodę, uwzględniając standard, normę lub inne wyspecyfikowane podejście, np. model National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

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;

2) 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;
3) 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;

4) wartość przetwarzanych informacji dla podmiotu nadzorowanego oraz skutki bezpośrednie i pośrednie utraty kontroli nad ich przetwarzaniem;
5) 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;
6) stanowisko nadzoru w sprawie tworzenia łańcucha outsourcingowego, zgodnie z którym:
   a) tworzenie łańcucha outsourcingowego powinno być każdorazowo oceniane przez podmiot nadzorowany z perspektywy przepisów szczególnych prawa dotyczących konkretnie realizowanych czynności przetwarzania informacji w chmurze obliczeniowej, a w szczególności:
      (i) tworzenie łańcucha outsourcingowego w zakresie działalności nadzorowanej jest dopuszczalne wyłącznie w granicach przewidzianych przepisami prawa;

(ii) tworzenie łańcucha outsourcingowego w zakresie innym niż w zakresie działalności nadzorowanej jest dopuszczalne, o ile nie jest wprost zakazane przez przepisy prawa lub postanowienia umowne;

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;

7) 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;

8) 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;

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

3. Podmiot nadzorowany w procesie szacowania ryzyka powinien uwzględnić potencjalną 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[3]. 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

1. Zarządzający posiadający licencję dokonuje szacowania ryzyka w udokumentowany sposób, zgodnie z metodyką opisaną w niniejszym Standardzie lub inną przyjętą przez niego metodyką.

    - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne wytyczne Powierzającego podmiotu nadzorowanego co do metodyki szacowania ryzyka, w tym katalogu ryzyk do oceny oraz czynników ryzyka wymagających uwzględnienia w związku z powierzeniem przetwarzania informacji w chmurze obliczeniowej. Zarządzający przekazuje Powierzającemu podmiotowi nadzorowanemu niezbędne informacje oraz wyniki szacowania ryzyka jako wkład do szacowania ryzyka przeprowadzanego przez Powierzający podmiot nadzorowany oraz na potrzeby wykazania przez Powierzający podmiot nadzorowany, że przetwarzanie informacji w chmurze obliczeniowej jest realizowane z uwzględnieniem postanowień Komunikatu i przepisów prawa. Ponadto Zarządzający przekazuje Powierzającemu podmiotowi nadzorowanemu informacje odnośnie wszelkich zmian w procesie chmurowym mogących wpłynąć na wyniki szacowania ryzyka.*

2. Zarządzający posiadający licencję powinien uwzględnić co najmniej te czynniki ryzyka, które wskazane zostały w Komunikacie.
3. W ramach szacowania ryzyka Zarządzający posiadający licencję ma obowiązek wziąć pod rozwagę także inne istotne zagrożenia wynikające z planowanego wykorzystania usług chmury obliczeniowej, jeżeli takie występują.
4. Wyniki szacowania ryzyka powinny dawać podstawę do twierdzenia, że świadczenie usługi chmury obliczeniowej będzie realizowane zgodnie z wymaganiami prawa, regulacjami zewnętrznymi i wewnętrznymi oraz standardami przyjętymi przez Zarządzającego posiadającego licencję.
5. Zarządzający posiadający licencję powinien nie rzadziej niż raz w roku zweryfikować czynniki mające istotny wpływ na szacowanie ryzyka (w tym wymogi o charakterze prawnym, regulacyjnym, organizacyjnym oraz technologicznym) i w razie konieczności dokonać ponownego szacowania ryzyka. W szczególności dotyczy to sytuacji zidentyfikowania nowych, nierozpoznanych dotychczas czynników ryzyka, które powinny być uwzględnione w toku procesu szacowania ryzyka przez Zarządzającego posiadającego licencję.
6. Czynniki, które Zarządzający posiadający licencję powinien uwzględnić w ramach szacowania ryzyka obejmują m.in. potencjalną możliwość przeanalizowania dostępnych wyników audytów zewnętrznych dostawców usług chmury obliczeniowej (VI.3.3) Komunikatu) oraz uprzedniego testowania usług chmury obliczeniowej, także przy wykorzystaniu scenariuszy warunków skrajnych

[3] Okresowa weryfikacja i aktualizacja powinna być prowadzona zgodnie z praktyką i zasadami podmiotu nadzorowanego, jednak nie rzadziej niż raz w roku.

(VI.3.4) Komunikatu). Za merytoryczną ocenę wyników audytów i testowanie usług chmury obliczeniowej, w tym opracowanie scenariuszy testów i ocenę ich wyników, odpowiedzialne powinny być osoby wyznaczone przez Zarządzającego posiadającego licencję zgodnie z jego regulacjami wewnętrznymi, posiadające kompetencje potwierdzone odpowiednią dokumentacją szkoleniową lub imiennymi zaświadczeniami w zakresie wymaganym do używanych usług chmury obliczeniowej. Mogą to być – przykładowo - członkowie departamentu bezpieczeństwa, departamentu IT, departamentu ryzyka lub compliance.

- *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający powinien, w przypadku występowania w tym zakresie instrukcji Powierzającego podmiotu nadzorowanego, weryfikować aktualność przeprowadzonego szacowania ryzyka, a w razie zidentyfikowania takiej konieczności (np. w związku ze zidentyfikowaniem nowych czynników ryzyka) poinformować o tym Powierzający podmiot nadzorowany i dokonać ponownego szacowania ryzyka – zgodnie z tymi instrukcjami.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO

1. Udokumentowany proces szacowania ryzyka pod kątem dopuszczalności przetwarzania informacji w chmurze obliczeniowej wraz z opisanym procesem okresowej weryfikacji oraz aktualizacji wyników szacowania ryzyka.
2. Dokument zawierający wyniki szacowania ryzyka usługi w chmurze obliczeniowej, uwzględniający strategię postępowania z ryzykiem (akceptacja, redukcja, przeniesienie lub unikanie) oraz plan postepowania z ryzykiem wraz z terminami i przypisanymi osobami odpowiedzialnymi za wdrożenie środków zaradczych.
3. Dokument potwierdzający formalne zatwierdzenie wyników szacowania ryzyka.
    - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający, zgodnie z instrukcjami Powierzającego podmiotu nadzorowanego, dokonuje oceny ryzyka usługi chmurowej i przekazuje Powierzającemu podmiotowi nadzorowanemu wszelkie niezbędne informacje oraz wyniki oceny ryzyka, mające stanowić wkład do oceny ryzyka przeprowadzanej przez Powierzający podmiot nadzorowany.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUGI CHMURY OBLICZENIOWEJ

1. Udokumentowane spełnienie wymagań w zakresie podstawowym z uwzględnieniem, w szczególności:
    1) niezbędnych kompetencji personelu dostawcy usług chmury obliczeniowej do planowanych lub prowadzonych działań przetwarzania informacji z wykorzystaniem usług chmurowych;
    2) lokalizacji CPD, obszaru przetwarzania danych (lokalizacji, z których personel dostawcy usług chmury obliczeniowej uzyskuje dostęp do danych Zarządzającego posiadającego licencję), przy czym dopuszczalne jest wskazanie w tym zakresie państwa oraz właściwego regionu;
    3) sposobu kontroli i monitorowania dostępu do przetwarzanych informacji przez personel dostawcy usług chmury obliczeniowej i jego poddostawców, w tym w szczególności dostępów uprzywilejowanych (kont administratorów, współadministratorów, serwisowych);

4) mechanizmów kontroli dostępu do usługi dla użytkowników, w szczególności MFA lub ograniczenia dostępu z urządzeń prywatnych;
5) opisu mechanizmów izolacji zasobów używanych do świadczenia usług chmury obliczeniowej wraz z informacją o potencjalnych skutkach awarii mechanizmów izolacji;
6) dokumentacji interfejsów zarządzających usługami chmury obliczeniowej, informacji o zabezpieczeniach interfejsów i ew. o ich podatnościach;
7) dokumentacji wykonywanych przeglądów, audytów lub kontroli, w tym testów bezpieczeństwa (częstotliwości, metodyki, zakresu, wyników, monitorowania statusów);
8) zasad uzgadniania wprowadzania zmian przez dostawcę usług chmury obliczeniowej;
9) możliwości kontrolowania dostawcy usług chmury obliczeniowej oraz jego poddostawców, w zakresie bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usług chmury obliczeniowej;
10) podziału odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy dostawcę usług chmury obliczeniowej a Zarządzającego posiadającego licencję;
11) monitorowania środowiska przetwarzania informacji w usłudze chmury obliczeniowej wraz z zasadami zarządzania logami;
12) możliwości integracji z innymi technologiami, które wskazane zostały przez Zarządzającego posiadającego licencję;
13) stosu technologicznego w zakresie zapewnienia bezpieczeństwa środowiska, danych (informacji) oraz zasobów chmury obliczeniowej, w szczególności mechanizmów szyfrowania i zarządzania kluczami szyfrującymi;
14) opracowanych i przetestowanych planów ciągłości działania oraz procedur odtworzeniowych, z uwzględnieniem mechanizmów redundancji oraz kopii bezpieczeństwa;
15) zasad zarządzania incydentami bezpieczeństwa;
16) łańcucha outsourcingowego, w tym procesu kontroli;
17) treść zawartych umów na korzystanie z usług chmury obliczeniowej lub, jeśli nie jest to możliwe, oparcie analizy na informacjach dostarczonych przez dostawcę usług chmury obliczeniowej

2. W przypadku analizy rozszerzonej zabezpieczeń można wykorzystać **Załącznik nr 8** do Standardu – Analiza ISO 27001.
3. Poinformowanie Zarządzającego posiadającego licencję o stosowanych zabezpieczeniach.
4. Udokumentowanie posiadanych certyfikatów lub ich odpowiedników, jeżeli to możliwe i uzasadnione:
   1) PN-ISO/IEC ISO 20000;
   2) PN-EN ISO/IEC 27001;
   3) PN-EN ISO 22301;
   4) ISO/IEC 27017;
   5) ISO/IEC 27018.

SZABLONY

1. **Załącznik nr 3** do Standardu – Przykład szablonu szacowania ryzyka
2. **Załącznik nr 8** do Standardu – Analiza ISO 27001

4. Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej.

1. Zapewnienie kompetencji

TREŚĆ KOMUNIKATU UKNF

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
   - 3.1. 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.
   - 3.2. 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.
   - 3.3. 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

1. Zarządzający posiadający licencję w celu zapewnienia bezpieczeństwa przetwarzanych w chmurze obliczeniowej informacji (lub co do których istnieje zamiar przetwarzania), powinien zapewnić właściwy poziom kompetencji pracowników i współpracowników, przy czym taki właściwy poziom kompetencji określa się, co do zasady, na podstawie wyników szacowania ryzyka. Utrzymanie i systematyczne podnoszenie kompetencji (kwalifikacji, wiedzy i umiejętności) powinno być częścią dobrych praktyk Zarządzającego posiadającego licencję. W przypadku stwierdzenia ewentualnych braków, należy je zaadresować poprzez stosowne nabycie kompetencji takich jak szkolenia zewnętrzne, wewnętrzne, przenoszenie wiedzy lub skorzystać ze wsparcia firm świadczących usługi konsultacyjno-doradcze w zakresie chmury obliczeniowej.
2. W zależności od Modelu usługi chmury obliczeniowej, Zarządzający posiadający licencję w udokumentowanym procesie powinien określić kompetencje w organizacji związane z przygotowaniem, realizacją oraz zakończeniem przetwarzania informacji w chmurze obliczeniowej.
   Przykładowymi kompetencjami w ramach wdrażania i utrzymania rozwiązań w publicznej chmurze obliczeniowej są:
   1) architektura (rola Architekt);
   2) bezpieczeństwo (rola Inżynier bezpieczeństwa);
   3) rozwój (rola Developer, Inżynier DevOps);
   4) utrzymanie (role Administrator, Administrator sieci, Inżynier DevOps);
   5) biznes (rola Opiekun biznesowy usługi);
   6) zgodność z wymaganiami prawnymi i umownymi (compliance).
3. Kompetencje powinny zapewniać bezpieczeństwo, spójność architektoniczną oraz dostarczać odpowiednie wsparcie rozwiązań, a także rozliczalność wykorzystywanych usług chmury obliczeniowej.
4. Kompetencje mogą być zapewnione przez podmioty zewnętrzne. Mimo tego Zarządzający posiadający licencję powinien posiadać kompetencje, które umożliwią kontrolę i nadzór nad podmiotami zewnętrznymi, którym zlecone zostało świadczenie usług. Zlecenie jakichkolwiek usług podmiotowi zewnętrznemu nie oznacza zwolnienia Zarządzającego posiadającego licencję z odpowiedzialności za jakość i bezpieczeństwo usług świadczonych między innymi na rzecz klientów oraz bezpieczeństwo ich danych.
5. Zarządzający posiadający licencję powinien posiadać aktywne wsparcie dostawcy usługi chmury obliczeniowej wraz z określonymi warunkami tego wsparcia w związku z przetwarzaniem informacji w chmurze obliczeniowej. Aktywne wsparcie dostawcy usługi chmury obliczeniowej w szczególności może polegać na współpracy w zakresie odpowiadania na wszelkie pytania i wątpliwości zarówno Zarządzającego, Powierzających podmiotów nadzorowanych jak i UKNF, wsparciu Zarządzającego w wykazywaniu wypełnienia wymagań – w szczególności poprzez

przekazywanie odpowiedniej dokumentacji, umożliwienie przeprowadzenia audytów, udzielanie wyjaśnień, a także reagowaniu na zmiany w przepisach prawa czy na nowe lub zmienione wytyczne organu nadzoru. Odpowiednie zobowiązania dostawcy usługi chmury obliczeniowej, określające zasady udzielania takiego aktywnego wsparcia, powinny zostać określone w umowie między Zarządzającym a dostawcą usługi chmury obliczeniowej.

- *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne wytyczne lub oczekiwania Powierzającego podmiotu nadzorowanego – w szczególności w zakresie (i) kompetencji – potwierdzonych odpowiednią dokumentacją szkoleniową lub imiennymi zaświadczeniami w zakresie odpowiednim do używanych usług chmury obliczeniowej (lub wynikających z umiejętności i doświadczenia), (ii) środowiska chmury obliczeniowej i Modelu usługi chmury obliczeniowej, (iii) infrastruktury teleinformatycznej, (iv) standardów ciągłości działania i bezpieczeństwa – oraz przekazuje mu niezbędne informacje w tym zakresie na potrzeby wykazania przez Powierzający podmiot nadzorowany, że przetwarzanie informacji jest realizowane z uwzględnieniem postanowień Komunikatu i przepisów prawa.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO

1. Udokumentowany proces zapewniający posiadanie przez Zarządzającego posiadającego licencję kompetencji wewnętrznych lub zewnętrznych niezbędnych do wdrożenia, utrzymania, rozwoju usług chmury obliczeniowej.
   - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego co do wkładu Zarządzającego w udokumentowanie kompetencji, w zakresie odpowiednim do wykorzystywanych usług chmury obliczeniowej, na potrzeby wykazania przez Powierzający podmiot nadzorowany, że przetwarzanie informacji jest realizowane z uwzględnieniem postanowień Komunikatu i przepisów prawa.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

1. Udokumentowane kompetencje.
2. Udokumentowane wsparcie dostawcy usług chmury obliczeniowej na rzecz Zarządzającego posiadającego licencję.

SZABLONY

N/D

2. Umowa z dostawcą usług chmury obliczeniowej

TREŚĆ KOMUNIKATU UKNF

4. **Umowa z dostawcą usług chmury obliczeniowej** 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[4] tam, gdzie to zasadne) oraz deklarowanego SLA wraz z metodą pomiaru i raportowania;
   b) klarowną definicję i wskazanie lokalizacji[5] 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;

---

[4] RTO – Recovery Time Objective, czas od momentu awarii systemu teleinformatycznego do momentu przywrócenia jego normalnego działania.
RPO – Recovery Point Objective, maksymalny czas pomiędzy wykonaniem kopii zapasowej informacji a momentem wystąpienia awarii usługi chmury obliczeniowej. Oznacza również potencjalną i akceptowaną przez podmiot nadzorowany możliwość utraty wyników przetwarzania informacji przez wskazany czas.

[5] Precyzyjne wskazanie lokalizacji centrum przetwarzania danych (CPD) może rodzić zagrożenie dla bezpieczeństwa fizycznego przetwarzanych informacji, jednak jako minimum należy operować pojęciami „strefa dostępu", „region" lub innymi równoważnymi, z podaniem co najmniej kraju oraz przybliżonej lokalizacji CPD, którymi dostawca usług chmury obliczeniowej posługuje się w standardowej komunikacji, np. podając miejscowość lub region kraju. W sytuacji, gdy takie określenie nie jest możliwe lub – z uwagi na skalę działania i liczbę miejsc przetwarzania informacji – jest niezasadne, należy podać obszar EOG (dla Europejskiego Obszaru Gospodarczego) lub inne równoważne określenie.

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

1. Zarządzający posiadający licencję zawiera sformalizowaną umowę z dostawcą usług chmury obliczeniowej.
2. Prawem właściwym dla umowy powinno być 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:
   1) postanowień umowy;
   2) wszystkich wymogów prawa polskiego ciążących na Zarządzającym posiadającym licencję;
   3) wytycznych organu nadzoru, w tym również w zakresie Komunikatu.
3. W przypadku poddania umowy prawu państwa trzeciego, Zarządzający posiadający licencję powinien posiadać pisemną opinię prawną, m.in. opracowaną przez wyspecjalizowany, niezależny od dostawcy usług chmury obliczeniowej podmiot, która może zostać przygotowana na zlecenie dostawcy Podmiotu nadzorowanego, potwierdzającą, że zgodnie z wybranym prawem właściwym umowy, wszystkie postanowienia umowy pomiędzy Zarządzającym posiadającym licencję a dostawcą usług chmury obliczeniowej spełniają wymagania prawa oraz wymagania Komunikatu, obowiązujące Zarządzającego posiadającego licencję.
   - *W ramach **Pośredniego stosowania Komunikatu** Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego co do modelu kontraktowania z dostawcą usług chmurowych. Zarządzający w szczególności bierze pod uwagę wytyczne Powierzającego podmiotu nadzorowanego w zakresie prawa właściwego umowy, a w przypadku poddania umowy prawu państwa trzeciego – zapewnia Powierzającemu podmiotowi nadzorowanemu niezbędne wsparcie w zakresie przygotowania pisemnej opinii prawnej zgodnie z rozdziałem VI.2.8) Komunikatu.*
4. Umowa z dostawcą usług chmury obliczeniowej powinna zawierać elementy wymienione w rozdziale VII.4.1 Komunikatu lub wskazywać ich źródła, które są zasadne w odniesieniu do używanych usług i zakresu przetwarzanych informacji w chmurze obliczeniowej. Dodatkowo, zgodnie z punktem VII.4.2 Komunikatu, Zarządzający posiadający licencję może korzystać z ramowych umów udostępnianych przez dostawców usług chmury obliczeniowej, przy założeniu braku uszczerbku dla wymagań prawa oraz z uwzględnieniem postanowień Komunikatu.
5. Zarządzający posiadający licencję powinien w umowie z dostawcą usług chmury obliczeniowej określić zasady i terminy rozwiązywania umowy oraz zwrotu danych, jak i trwałego i bezpiecznego usunięcia informacji przez dostawcę z infrastruktury dostawcy i podmiotów z nim współpracujących.
6. W trakcie trwania umowy i po zakończeniu współpracy z dostawcą usług chmury obliczeniowej Zarządzający posiadający licencję powinien zapewnić sobie pełną i wyłączną kontrolę nad danymi

i informacjami uzyskanymi w wyniku przetwarzania danych dostarczonych przez Zarządzającego posiadającego licencję, np. profilami behawioralnymi (informacje).

- *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający powinien uwzględnić, że Powierzający podmiot nadzorowany zobowiązany jest do zapewnienia, że przetwarzanie informacji jest realizowane z uwzględnieniem postanowień Komunikatu. W praktyce, w przypadku outsourcingu łańcuchowego, odpowiednie uwzględnienie obszarów kontraktowych wskazanych w rozdziale VII.4.1 Komunikatu powinno być zweryfikowane w ramach całego łańcucha umów.*
- *Zarządzający w umowie z dostawcą usług chmury obliczeniowej (oraz innych dokumentach) uwzględnia wymogi rozdziału VII.4.1. Komunikatu co najmniej w zakresie niezbędnym do wykonania umowy z Powierzającym podmiotem nadzorowanym w związku z wykorzystywaniem chmury obliczeniowej w ramach wykonywania powierzonych Zarządzającemu czynności – w tym, w szczególności, w zakresie:*
  - *zasad tworzenia łańcucha outsourcingowego w granicach przewidzianych przepisami prawa, w tym możliwości lub braku możliwości korzystania przez Zarządzającego z poddostawców (dalszych dostawców dostawcy usług chmury obliczeniowej) i udzielania Powierzającemu podmiotowi nadzorowanemu informacji o poddostawcach;*
  - *zasad i terminów informowania o zamiarze wprowadzania zmian do umowy z dostawcą usług chmury obliczeniowej w tym parametrów technicznych usług chmury obliczeniowej;*
  - *odpowiedzialności (w szczególności za szkody wyrządzone klientom Powierzającego podmiotu nadzorowanego) i kar umownych;*
  - *uprawnień Zarządzającego, Powierzającego podmiotu nadzorowanego oraz organu nadzoru do przeprowadzenia inspekcji dostawcy usług chmury obliczeniowej oraz poddostawców;*
  - *zasad rozwiązania umowy z dostawcą usług chmury obliczeniowej;*
  - *lokalizacji informacji, zasad zwrotu i usunięcia oraz własności informacji po zakończeniu korzystania z usług chmury obliczeniowej przez Zarządzającego i podziału odpowiedzialności za bezpieczeństwo informacji;*
  - *zasad przetwarzania danych osobowych;*
  - *dokumentacji technicznej i deklaracji zgodności oraz zasad wsparcia,*

  oraz inne ewentualne oczekiwania Powierzającego podmiotu nadzorowanego co do sposobu i warunków korzystania z usług chmury obliczeniowej (w szczególności zdeterminowane obowiązkami regulacyjnymi Powierzającego podmiotu nadzorowanego).

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO

1. Umowa z dostawcą usług chmury obliczeniowej wraz niezbędnymi dokumentami (oświadczenia, regulaminy, warunki korzystania z usług, itp.).
   - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia potrzebę „odzwierciedlenia" w umowie z dostawcą usług chmurowych obowiązków nałożonych na Zarządzającego w umowie z Powierzającym podmiotem nadzorowanym – w szczególności wynikających z wymogów nadzorczych i prawnych wiążących Powierzający podmiot nadzorowany.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

1. Zawarcie z Zarządzającym posiadającym licencję umowy uwzględniającej wymagania Komunikatu i bezwzględnie obowiązujących przepisów prawa.

SZABLONY

N/D

3. Plan przetwarzania informacji w chmurze obliczeniowej

TREŚĆ KOMUNIKATU UKNF

5. **Plan przetwarzania informacji w chmurze obliczeniowej** 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

1. Zarządzający posiadający licencję w ramach planowanego i bieżącego przetwarzania informacji w chmurze obliczeniowej powinien posiadać udokumentowany plan przetwarzania informacji w chmurze obliczeniowej. Plan ten w szczególności powinien zawierać opis:
   1) zadania realizowanego za pomocą usługi chmury obliczeniowej, w tym opis przetwarzanych informacji w chmurze obliczeniowej z uwzględnieniem podziału na informacje prawnie chronione oraz inne informacje;
   2) stosowanych zabezpieczeń informacji (pseudonimizacja, anonimizacja), w tym opis schematu szyfrowania informacji i przechowywania kluczy szyfrujących, wraz z określeniem czy

szyfrowanie będzie wykonywane przy pomocy kluczy własnych, czy kluczy dostawcy usług chmury obliczeniowej oraz ze wskazaniem miejsca i sposobu przechowywania kluczy szyfrujących (w ramach infrastruktury własnej lub dostawcy usług chmury obliczeniowej);

3) relacji umownej z dostawcą usług chmury obliczeniowej, w tym wskazanie prawa właściwego dla umowy.

2. Plan przetwarzania informacji w chmurze obliczeniowej w oparciu o wewnętrzną klasyfikację informacji powinien precyzyjnie określać, jakie informacje Zarządzający posiadający licencję przetwarza w chmurze obliczeniowej w ramach konkretnego rozwiązania.
3. W planie przetwarzania informacji w chmurze obliczeniowej należy uwzględnić szczegółowy opis zasad kontroli przyznawania dostępu do danych, wskazujący grupy osób upoważnionych w tym przedmiocie, wraz z określeniem poziomu uprawnień przysługujących poszczególnym osobom.
4. Plan przetwarzania informacji w chmurze obliczeniowej powinien być przeglądany w ustalonych cyklach bądź przy wystąpieniu większych zmian w zakresie lub sposobie przetwarzania informacji w chmurze obliczeniowej.
    - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego odnośnie do udzielenia wsparcia w opracowaniu planu przetwarzania informacji w chmurze obliczeniowej, w tym przekazania niezbędnych informacji. Zarządzający w szczególności powinien wziąć pod uwagę wytyczne Powierzającego podmiotu nadzorowanego w zakresie (i) umowy z dostawcą usługi chmurowej oraz (ii) stosowanych mechanizmów zabezpieczania informacji, w tym kontroli dostępu do informacji należących do Powierzającego podmiotu nadzorowanego.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO POSIADAJĄCEGO LICENCJĘ

1. Plan przetwarzania informacji w chmurze obliczeniowej.

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

N/D

SZABLONY

Załącznik nr 5 do Standardu – Wzorcowy plan przetwarzania informacji w chmurze obliczeniowej

TREŚĆ KOMUNIKATU UKNF

5.2 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

1. Przed uruchomieniem produkcyjnym Zarządzający posiadający licencję, o ile jest to zasadne w przypadku konkretnych usług chmury obliczeniowej, powinien przeprowadzić i udokumentować przeprowadzenie testów usługi chmury obliczeniowej.
2. Testy powinny być przeprowadzone na danych testowych (generowanych maszynowo lub w inny przypadkowy sposób), które w szczególności nie zawierają danych osobowych ani informacji prawnie chronionych.
3. Przeprowadzone testy powinny być adekwatne do oszacowanego ryzyka, skali, krytyczności danych i procesu uruchomionego w chmurze obliczeniowej lub w oparciu o chmurę obliczeniową (zgodnie rozdziału VI. Komunikatu – Wytyczne do szacowania ryzyka). W oparciu o wyniki szacowania ryzyka, Zarządzający posiadający licencję może zdecydować o braku konieczności realizacji testów. Zarządzający posiadający licencję powinien w takim przypadku uzasadnić i udokumentować decyzję o braku konieczności realizacji testów.
4. Adekwatnie do Modelu usługi chmury obliczeniowej, scenariusze testowe należy przygotować także w sytuacji, w której Zarządzający posiadający licencję nie posiada bezpośredniej relacji umownej z dostawcą usług chmury obliczeniowej.
    - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego odnośnie do sposobu przeprowadzenie testów usługi chmury obliczeniowej, a także – jeśli będzie to zasadne – przekazuje wyniki tych testów lub uzasadnia brak konieczności ich realizacji.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO POSIADAJĄCEGO LICENCJĘ

1. Udokumentowane wyniki testów lub uzasadnienie decyzji o braku konieczności realizacji testów.

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

N/D

SZABLONY

N/D

TREŚĆ KOMUNIKATU UKNF

5.3 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

1. Zarządzający posiadający licencję opracowuje udokumentowany i przetestowany plan wycofania się z przetwarzania informacji w ramach usługi chmury obliczeniowej (tj. plan wyjścia) zarówno w sytuacji zmiany strategii, jak i w sytuacji awaryjnej.
2. Plan wyjścia powinien być adekwatny do oszacowanego ryzyka, skali, krytyczności danych i procesu uruchomionego w chmurze obliczeniowej lub w oparciu o chmurę obliczeniową. Zarządzający posiadający licencję powinien zidentyfikować, z jakich procesów i aplikacji korzysta, w tym:
   1) zbadać, w szczególności z uwzględnieniem rozdziału VI.2.1.e i h Komunikatu, które z tych procesów i aplikacji mają istotny wpływ na działalność Zarządzającego posiadającego licencję oraz które procesy i aplikacje mogą zostać przeniesione do innych dostawców usługi chmury obliczeniowej lub do infrastruktury „on-premise”;
   2) dokonać kwalifikacji (w oparciu o szacowanie ryzyka), czy dany proces i aplikacja ma istotne znaczenie.
3. Plan wyjścia powinien zapewnić, że w sytuacji awaryjnej nie dojdzie do uszczerbku dla zachowania zgodności działania Zarządzającego posiadającego licencję z wymaganiami prawa i innymi regulacjami, w tym związanymi z udzielonymi licencjami lub zezwoleniami na prowadzenie określonej działalności.
4. Plan wyjścia powinien określać dalsze niezbędne czynności, mające na celu zabezpieczenie ciągłości bieżącego działania po zakończeniu współpracy z dostawcą usługi chmury obliczeniowej, obejmujące w szczególności:
   1) zwrot danych lub ich migrację do wskazanego w planie wyjścia alternatywnego dostawcy usług chmury obliczeniowej;
      lub
   2) powrót danych, w pełnym albo ograniczonym zakresie, do środowiska „on-premise”.
5. Plan wyjścia powinien być przetestowany, przy czym zakres i podejście do testów powinny wynikać z analizy ryzyka (zgodnie z rozdziałem VI. Komunikatu – Wytyczne do szacowania ryzyka) w oparciu o obowiązujące u Zarządzającego posiadającego licencję metodyki.
6. Testy planu wyjścia:
   1) powinny obejmować procesy i aplikacje, które mają istotny wpływ na działalność Zarządzającego posiadającego licencję, a nie na dostawcę usług chmury obliczeniowej. Testowanie nie powinno być ograniczone do teoretycznych ćwiczeń symulujących podjęcie adekwatnych kroków w przypadku wystąpienia określonych zdarzeń (np. przeprowadzenia gry sztabowej);
   2) powinny być realizowane w terminach i w oparciu o obowiązujące u Zarządzającego posiadającego licencję metodyki, w szczególności poprzez rzeczywiste wykonanie działań awaryjnych w stosunku do procesów i aplikacji, które mają istotny wpływ na działalność Zarządzającego posiadającego licencję, przy czym zalecane jest testowanie planu wycofania nie rzadziej niż raz w roku;
   3) powinny odbywać się rotacyjnie w oparciu o różne procesy i aplikacje. Rotacyjne testowanie powinno dotyczyć procesów i aplikacji, które mają istotny wpływ na działalność Zarządzającego posiadającego licencję.
7. Plan wyjścia powinien być przeglądany i aktualizowany w okresie określonym przez wewnętrzne procedury Zarządzającego posiadającego licencję.

8. Plan wyjścia powinien zawierać kryteria podjęcia decyzji o jego uruchomieniu, w szczególności powinien uwzględniać:
   1) opcję długo oraz średnioterminową – przejawiającą się m.in. w:
      a) obniżeniu jakości usług lub pogorszeniu kondycji finansowej Dostawcy;
      b) nieakceptowalnej zmianie warunków świadczenia usługi przez Dostawcę;
      c) wypowiedzeniu umowy przez Dostawcę;
      d) wewnętrznej decyzji biznesowej o zaprzestaniu korzystania z usługi lub zmiany strategii korzystania z usług zewnętrznych Dostawców;
      e) decyzji administracyjnej nakazującej Zarządzającemu posiadającemu licencję rozwiązanie umowy z Dostawcą.
   2) opcję krótkoterminową – związaną z:
      a) wystąpieniem sytuacji awaryjnej wynikającej z utrzymującej się niedostępności usług przez okres dłuższy niż przewidziany w odpowiednich regulacjach wewnętrznych oraz brakiem perspektyw na przywrócenie normalnego funkcjonowania tych usług;
      b) nagłym zaprzestaniem działalności przez Dostawcę;
      c) wystąpieniem poważnego incydentu skutkującego naruszeniem bezpieczeństwa usług i powierzonych danych.

- *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego odnośnie do opracowania planu wyjścia.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO POSIADAJĄCEGO LICENCJĘ

1. Plan wycofania się z usługi chmury obliczeniowej.
2. Scenariusze testowe dla planu wycofania się z usługi chmury obliczeniowej.

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

N/D

SZABLONY

1. **Załącznik nr 6** do Standardu – Wzorcowy szablon scenariusza wyjścia z chmury

TREŚĆ KOMUNIKATU UKNF

5.4	Podmiot nadzorowany powinien posiadać udokumentowany plan ciągłości działania uwzględniający potencjalną 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

1. Zarządzający posiadający licencję, stosowanie do wyników przeprowadzonej oceny ryzyka, uwzględnia wykorzystanie usługi chmury obliczeniowej w planie ciągłości działania oraz planach awaryjnych, zapewniając np. alternatywne wobec Dostawcy miejsce przechowywania kopii zapasowych danych o znaczeniu krytycznym.
2. Zarządzający posiadający licencję posiada udokumentowany plan ciągłości działania uwzględniający m.in.:
   1) możliwość utraty kontroli nad informacjami przetwarzanymi w chmurze obliczeniowej; oraz
   2) ryzyko przerwania ciągłości działania usługi.
3. W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej chmur obliczeniowych lub dwóch lub więcej dostawców usług chmury obliczeniowej, Zarządzający posiadający licencję powinien regularnie weryfikować możliwość realizacji zakładanego scenariusza, zwłaszcza po zmianach w obszarze technologicznym u co najmniej jednego z dostawców usług chmury obliczeniowej.
4. W uzasadnionych przypadkach, gdy poziom krytyczności procesu wspieranego przez usługę chmury obliczeniowej nie ma istotnego wpływu na działalność Zarządzającego posiadającego licencję, dopuszcza się rezygnację z opracowywania planu ciągłości działania.
   - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego odnośnie do opracowania planu ciągłości działania i udostępniania tego planu (zarówno własnego jak i planu ciągłości działania dostawcy usługi chmurowej).*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO POSIADAJĄCEGO LICENCJĘ

1. 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 usług chmury obliczeniowej;
   2) możliwości przerwania ciągłości działania usługi chmury obliczeniowej.
2. Dokumentacja związana z planowaniem ciągłości działania zgodnie z metodyką przyjętą u Zarządzającego posiadającego licencję (zawierająca w szczególności wyniki testów ciągłości działania).
3. W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej chmur obliczeniowych lub dwóch lub więcej dostawców usług chmury obliczeniowej:

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 pkt. 3.1) powyżej, w szczególności dotyczące weryfikacji możliwości realizacji scenariusza po zmianach technologicznych u jednego z dostawców usług chmury obliczeniowej.

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

N/D

SZABLONY

1. **Załącznik nr 9** do Standardu – Wytyczne do opracowania planu ciągłości działania.

4. Wymagania dla dostawców usług chmury obliczeniowej

TREŚĆ KOMUNIKATU UKNF

6. Wymagania dla dostawców usług chmury obliczeniowej[6]

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] Wymagania te uwzględnia podmiot nadzorowany w swoim podejściu do stosowania usług chmury obliczeniowej, a w szczególności w procesie szacowania ryzyka.

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

OPIS WYMAGAŃ

1. Zarządzający posiadający licencję, w zależności od Modelu usługi chmury obliczeniowej oraz z uwzględnieniem wyników klasyfikacji i oceny informacji, podejmuje decyzję dotyczącą oczekiwanego zakresu wdrożenia zabezpieczeń przez dostawcę usług chmury obliczeniowej w modelu:
   1) podstawowym – w takim przypadku Zarządzający posiadający licencję weryfikuje zabezpieczenia w oparciu o zakres przedstawiony w pkt. 1 sekcji *działania do podjęcia / produkty do opracowania po stronie dostawcy usług chmury obliczeniowej* dotyczącej rozdziału VI. Komunikatu – Wytyczne do szacowania ryzyka lub
   2) rozszerzonym – w takim przypadku Zarządzający posiadający licencję weryfikuje zabezpieczenia w oparciu o wymagania zawarte w Załączniku A standardu ISO 27001, w oparciu o szablon przedstawiony w Załączniku nr 6 do Standardu – Wzorcowy szablon scenariusza wyjścia z chmury
2. Niezależnie od wybranego katalogu zabezpieczeń, w zależności od Modelu usługi chmury obliczeniowej oraz przy zachowaniu zasady proporcjonalności, Zarządzający posiadający licencję może zmienić katalog weryfikowanych zabezpieczeń.
3. W zależności od decyzji Zarządzającego posiadającego licencję, dostawca usług chmury obliczeniowej powinien zapewnić zgodność usługi chmury obliczeniowej z normami ISO wymienionym w rozdziale VII 6.1 i 6.2 Komunikatu lub ich odpowiednikami (normami BS, normami PN-ISO, etc.).
4. Zapewnienie zgodności może być realizowane poprzez uzyskanie przez dostawcę usług chmury obliczeniowej niezależnej certyfikacji (wydanej przez jednostkę certyfikującą); w przypadku, gdy dostawca usług chmury obliczeniowej nie posiada formalnej certyfikacji, powinien on wykazać zgodność z ww. normami poprzez udokumentowanie realizacji poszczególnych wymagań norm.
5. Dokumentacja związana ze zgodnością oraz wyniki audytów certyfikacyjnych powinny być przekazane przez dostawcę usług chmury obliczeniowej przed zawarciem umowy oraz udostępniane na żądanie Zarządzającego posiadającego licencję. Zasady udostępniania ww. dokumentacji i wyników audytów powinny zostać określone w umowie z dostawcą usługi chmury obliczeniowej.
6. Zarządzający posiadający licencję powinien regularnie weryfikować ww. dokumentację i wyniki audytów, a w przypadku, gdy weryfikacja wykaże istotne niezgodności, Zarządzający posiadający licencję powinien uzgodnić z dostawcą usług chmury obliczeniowej plan naprawczy oraz monitorować jego realizację.
   - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego co do zakresu stosowanych zabezpieczeń przez dostawcę usług chmury obliczeniowej oraz zgodności usługi chmury obliczeniowej z normami ISO wymienionymi w rozdziale VII 6.1 i 6.2 Komunikatu lub ich odpowiednikami.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO

1. Udokumentowane wymagania Zarządzającego posiadającego licencję w zakresie ww. norm i standardów, w szczególności dokumentacja akceptacji ryzyka w przypadku rezygnacji z wybranych wymagań.
2. Pozyskanie certyfikacji dostawcy usług chmury obliczeniowej lub innej dokumentacji zgodności dostawcy usług chmury obliczeniowej z wymaganiami Komunikatu.
3. Udokumentowany proces oceny dokumentacji związanej z certyfikacją lub zgodnością z Komunikatem, jeżeli ma zastosowanie.
    - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający przekazuje Powierzającemu podmiotowi nadzorowanemu informacje odnośnie do weryfikacji zabezpieczeń, dokumentacji związanej ze zgodnością oraz wyniki audytów certyfikacyjnych.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

1. Certyfikacja zgodnie z normami ISO wymienionym w pkt VII ust. 6.1 i 6.2 Komunikatu, obejmująca zakresem usługę świadczoną na rzecz Zarządzającego posiadającego licencję lub dokumentacja zgodności z przedmiotowymi normami przygotowana przez dostawcę usług chmury obliczeniowej.

SZABLONY

N/D

TREŚĆ KOMUNIKATU UKNF

6.3. 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

1. Rekomendowany jest wybór dostawców usług chmury obliczeniowej oferujących CPD na terenie EOG, należy jednak mieć na względzie, że nie wyklucza to jednoznacznie ryzyka przetwarzania danych przez dostawcę usług chmury obliczeniowej poza EOG.
2. W przypadku gdy CPD zlokalizowane jest na terenie EOG, Zarządzający posiadający licencję korzystający z usług chmury obliczeniowej globalnego dostawcy usług chmury obliczeniowej powinien określić odpowiednie mechanizmy kontrolne w tym zakresie.
3. W przypadku gdy CPD zlokalizowane jest na terenie EOG, ale usługa jest również wspierana przez personel lub poddostawców mających dostęp do danych zlokalizowany poza EOG, wymagane jest wdrożenie odpowiednich zabezpieczeń i zapewnienie zgodności z przepisami w tym zakresie. Zabezpieczenia te powinny uwzględniać trzy obszary, tj.:
   1) kontraktowy, w tym włączenie do umów z Dostawcami postanowień określających sposoby monitorowania lokalizacji przetwarzania danych w chmurze obliczeniowej, zakres i zasady dostępu poddostawców do danych, metody ograniczenia identyfikowanego dostępu do danych, jeśli ich funkcjonowanie zapewnia Dostawca;
   2) technologiczny, w tym zapewnienie szyfrowania informacji przetwarzanych w chmurze obliczeniowej, przeglądu logów;
   3) organizacyjny obejmujący wdrożenie i utrzymanie procedur wewnętrznych służących m.in. monitorowaniu realizacji rozwiązań przyjętych na potrzeby spełnienia wymagań wynikających z Komunikatu chmurowego UKNF.
   - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego w zakresie lokalizacji – zarówno CPD jak i lokalizacji przetwarzania przez osoby trzecie, np. pracowników (współpracowników) oraz poddostawców dostawcy usług chmury obliczeniowej.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO

1. Jednoznaczne wskazanie lokalizacji CPD (co najmniej kraj, region lub miejscowość) wykorzystywanych w usłudze.
2. W przypadku gdy uzasadniony jest wybór CPD poza EOG, udokumentowana analiza ryzyka uzasadniająca taką decyzję.
   - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający przekazuje Powierzającemu podmiotowi nadzorowanemu informacje odnośnie do lokalizacji CPD i weryfikacji zabezpieczeń CPD oraz przetwarzanych informacji.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

1. Jednoznaczne wskazanie wszystkich lokalizacji CPD (co najmniej kraj, region lub miejscowość) wykorzystywanych w poszczególnych usługach (w formie oświadczenia dostawcy usługi chmury obliczeniowej).

SZABLONY

N/D

TREŚĆ KOMUNIKATU UKNF

6.4.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[7] 2 Type 2) wydanym przez niezależną jednostkę certyfikującą akredytowaną w europejskim systemie akredytacji;
d) udostępnienie wytycznych, wzorcowych konfiguracji, opisów zasadtd.tp., 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"[8].

OPIS WYMAGAŃ

1. Dostawca usługi chmury obliczeniowej powinien zapewnić Zarządzającemu posiadającemu licencję mechanizm kontroli udzielania dostępu do danych przetwarzanych w usłudze chmury obliczeniowej, w tym dla pracowników (współpracowników) i poddostawców dostawcy usług chmury obliczeniowej.

[7] System and Organization Controls.

[8] Oznacza domyślną konfigurację usługi chmury obliczeniowej, która uwzględnia wymagania bezpieczeństwa przetwarzania informacji, w szczególności zapobiega przypadkowemu (niezamierzonemu) ujawnieniu przetwarzanej informacji.

2. W zależności od Modelu usługi chmury obliczeniowej i w miarę możliwości technologicznych, dostawca usług chmury obliczeniowej nie powinien mieć stałego dostępu do danych ani dostępu administracyjnego, serwisowego itd. na poziomie serwerów, baz danych, aplikacji czy urządzeń.
3. Dostawca usługi chmury obliczeniowej powinien zapewnić Zarządzającemu posiadającemu licencję dostęp do dokumentacji potwierdzającej separację tenantów, dokumentacji mechanizmów zapewniających poprawność separacji lub oświadczenia stosowania takich mechanizmów.
4. Nowo uruchamiane usługi powinny być domyślnie odseparowane (od momentu uruchomienia) i skonfigurowane zgodnie z najlepszymi praktykami bezpieczeństwa (hardening).
   - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego w zakresie:*
     - *udzielania dostępu do danych dla pracowników (współpracowników) i poddostawców dostawcy usług chmury obliczeniowej oraz lokalizacji przetwarzania;*
     - *udostępniania odpowiedniej dokumentacji technicznej zgodnie z wymogami Komunikatu.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO

1. Potwierdzenie stosowania ww. mechanizmów w postaci dokumentacji technologicznej lub oświadczeń dostawcy usług chmury obliczeniowej.
   - *W ramach Pośredniego stosowania **Komunikatu**, Zarządzający przekazuje Powierzającemu podmiotowi nadzorowanemu informacje dotyczące ww. mechanizmów.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

1. Potwierdzenie stosowania ww. mechanizmów w postaci dokumentacji technologicznej lub oświadczeń.

SZABLONY

N/D

5. Kryptografia

TREŚĆ KOMUNIKATU UKNF

7. 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

1. Informacje przetwarzane w chmurze obliczeniowej muszą być szyfrowane. Mechanizmy i zakres wykorzystywania zabezpieczeń kryptograficznych powinny wynikać z analizy ryzyka z zachowaniem zasady proporcjonalności (zgodnie z rozdziałem VI ust. 5.2 Komunikatu). W szczególności wymagane jest:
   1) szyfrowanie zarówno podczas przesyłu, jak i podczas spoczynku („at rest" jak i „in transit") Informacji prawnie chronionej;
   2) przekazanie do Zarządzającego posiadającego licencję informacji, a także mechanizmów weryfikacji poprawności konfiguracji i działania w/w mechanizmów;
   3) posiadanie przez Zarządzającego posiadającego licencję kompetencji w zakresie poprawnej konfiguracji usług chmury obliczeniowej, w tym mechanizmów szyfrowania;
   4) w zależności od Modelu usługi chmury obliczeniowej korzystanie z zalecanych ustawień podnoszących bezpieczeństwo (tzw. hardening); ustawienia te powinny zostać udokumentowane.
   - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia oczekiwania Powierzającego podmiotu nadzorowanego w zakresie zasad szyfrowania informacji przetwarzanych w chmurze obliczeniowej, w szczególności w przypadku przetwarzania w chmurze obliczeniowej Informacji prawnie chronionych.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO POSIADAJĄCEGO LICENCJĘ

Z uwzględnieniem Modelu usługi chmury obliczeniowej:

1. dokumentacja mechanizmów szyfrowania oraz metody weryfikacji poprawności konfiguracji szyfrowania;
2. potwierdzenie posiadanych kompetencji – patrz pkt VII.3 Komunikatu;
3. dokumentacja hardeningu usługi, w szczególności uwzględniająca wykorzystanie mechanizmów szyfrowania;

4. potwierdzenie szyfrowania danych (informacji) w spoczynku i podczas przesyłu (w szczególności informacje przekazane przez dostawcę usług chmury obliczeniowej, dokumentacja techniczna etc.).

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

1. Potwierdzenie stosowania w/w mechanizmów w postaci dokumentacji technologicznej lub oświadczeń dostawcy usług chmury obliczeniowej.

SZABLONY

N/D

TREŚĆ KOMUNIKATU UKNF

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.

7.3. W przypadku, gdy z szacowania ryzyka wynika konieczność utrzymywania i zarządzania kluczami szyfrującymi przy wykorzystaniu sprzętowych rozwiązań (HSM[9]), to HSM mogą być udostępniane przez dostawcę usług chmury obliczeniowej, przy uwzględnieniu tego elementu w szacowaniu ryzyka. HSM powinny spełniać wymagania minimum FIPS[10] 140-2 Level 2 lub równoważne.

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

[9] HSM – Hardware Security Module, urządzenie do przechowywania i zarządzania kluczami kryptograficznymi

[10] Federal Information Processing Standard – publiczne standardy dla agencji cywilnych i rządowych w USA. W tym przypadku międzynarodowy standard bezpieczeństwa dla systemów kryptograficznych.

1. W zależności od Modelu usługi chmury obliczeniowej lub o ile ma to uzasadnienie w ocenie ryzyka, Zarządzający posiadający licencję powinien zapewnić, że informacje są szyfrowane kluczami generowanymi oraz zarządzanymi przez Zarządzającego posiadającego licencję. Brak spełnienia tego wymogu powinien zostać poparty wnioskami wynikającymi z szacowania ryzyka.
2. W zależności od Modelu usługi chmury obliczeniowej, proces zarządzania tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących powinien być udokumentowany i posiadać określone mechanizmy kontrolne.
3. W zależności od Modelu usługi chmury obliczeniowej, w przypadku wykorzystania kluczy wygenerowanych lub zarządzanych przez dostawcę, Zarządzający posiadający licencję powinien zapewnić, że proces wspomniany w pkt. 2 powyżej zapewnia przechowywanie kopii kluczy w infrastrukturze Zarządzającego posiadającego licencję, chyba że analiza ryzyka uzasadnia brak takiego mechanizmu.
4. W zależności od wyników szacowania ryzyka, możliwe jest stosowanie technologii HSM. HSM może być udostępniony przez dostawcę usług chmury obliczeniowej lub być zarządzany przez Zarządzającego posiadającego licencję. Bez względu na to, która strona udostępnia HSM, musi on spełniać wymagania FIPS 140-2 Level 2 lub równoważne.
    - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego dotyczące kluczy szyfrujących służących do szyfrowania informacji w chmurze obliczeniowej.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO POSIADAJĄCEGO LICENCJĘ

Z uwzględnieniem Modelu usługi chmury obliczeniowej:

1. dokumentacja techniczna potwierdzająca, że informacje są szyfrowane kluczami generowanymi / dostarczonymi oraz zarządzanymi przez Zarządzającego posiadającego licencję;
2. w przypadku, gdy pkt. 1 powyżej nie jest spełniony, analiza ryzyka z której wynika dopuszczalność używania kluczy szyfrujących generowanych/dostarczonych i zarządzanych przez Dostawcę.
3. udokumentowany proces zarządzania tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących oraz przechowywaniem kopii zapasowych kluczy w infrastrukturze Zarządzającego posiadającego licencję;
4. w przypadku, gdy proces zarządzania kluczami szyfrującymi nie zapewnia przechowywania kopii kluczy w infrastrukturze Zarządzającego posiadającego licencję, analiza ryzyka z której wynika uzasadniony brak takiej potrzeby;
5. dokumentacja potwierdzająca spełnienie wymagania FIPS 140-2 Level 2 lub równoważnego, jeśli wykorzystywany jest HSM.

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

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

2. Dokumentacja potwierdzająca spełnienie wymagania FIPS 140-2 Level 2 lub równoważnego, jeśli wykorzystywany jest HSM.

SZABLONY

N/D

6. Monitorowanie środowiska przetwarzania informacji w usługach chmury obliczeniowej

TREŚĆ KOMUNIKATU UKNF

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

1. Istotnym elementem związanym z wykorzystaniem usług przetwarzania informacji w chmurze obliczeniowej jest kwestia monitorowania środowiska przetwarzania informacji w usłudze chmury obliczeniowej.
2. Zgodnie z wytycznymi Komunikatu, w zakresie monitorowania środowiska przetwarzania informacji w usłudze chmury obliczeniowej oraz w zależności od Modelu usługi chmury obliczeniowej Zarządzający posiadający licencję lub dostawca usług chmury obliczeniowej 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, liczby logów, stosowanych przez Zarządzającego posiadającego licencję rozwiązań technicznych, etc. Można rozważyć przekazywanie logów do systemu klasy SIEM oraz opracowanie reguł korelacji pozwalających na wykrycie incydentu bezpieczeństwa w chmurze obliczeniowej.
   - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego w zakresie zasad zbierania i zabezpieczania logów związanych z przetwarzaniem informacji w chmurze obliczeniowej.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO POSIADAJĄCEGO LICENCJĘ

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

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

1. Dokumentacja w zakresie logowania zdarzeń w chmurze obliczeniowej, a także możliwości integracji mechanizmów logowania w chmurze obliczeniowej z systemem klasy SIEM, jeżeli są wykorzystywane przez Zarządzającego posiadającego licencję.

SZABLONY

N/D

TREŚĆ KOMUNIKATU UKNF

8.4. Wymagania w stosunku do podmiotu nadzorowanego w zakresie zarządzania dostawcami usług mającymi dostęp zdalny do usług chmury obliczeniowej wykorzystywanych przez podmiot nadzorowany[11]:

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

[11] 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). Wymagania te nie dotyczą usług wsparcia świadczonych przez dostawcę usług chmury obliczeniowej w zakresie standardów obsługi wynikających z umowy na świadczenie usług chmury obliczeniowej.

parametrów, a następnie poprzez analizowanie prawidłowości i celowości realizowanych czynności), chyba że z szacowania ryzyka wynika uzasadniony brak takiej potrzeby.

OPIS WYMAGAŃ

1. Zarządzający posiadający licencję powinien zapewnić poprzez mechanizmy kontrolne lub postanowienia umowne, że dostęp do systemów wykorzystywanych w usłudze chmury obliczeniowej ma wyłącznie uprawniony personel po stronie Dostawcy.
2. Dostęp personelu Dostawcy usług do systemów wykorzystywanych w chmurze obliczeniowej powinien być zabezpieczony przez silne, wieloskładnikowe uwierzytelnienie, zgodnie z zachowaniem zasady proporcjonalności i wynikami analizy ryzyka.
3. Personel Dostawcy powinien uzyskiwać dostęp (w przypadku dostępu administracyjnego lub o charakterze uprzywilejowanym) wyłącznie z dedykowanych i zabezpieczonych stacji roboczych/terminali, zlokalizowanych w bezpiecznej (zaufanej) lokalizacji sieciowej.
    - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego w zakresie dalszego ujawniania informacji prawnie chronionych i modelu zabezpieczenia tych informacji w ramach całego łańcucha outsourcingowego.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO POSIADAJĄCEGO LICENCJĘ

Z uwzględnieniem Modelu usługi chmury obliczeniowej:

1. udokumentowane procedury lub postanowienia umowne potwierdzające zasady dostępu do informacji Zarządzającego posiadającego licencję przez uprawniony personel dostawcy;
2. opis mechanizmów uwierzytelnienia w zakresie dostępu personelu Dostawcy.

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

Z uwzględnieniem Modelu usługi chmury obliczeniowej:

1. używanie przez personel dostawcy, mający dostęp zdalny do systemów wykorzystywanych w usłudze chmury obliczeniowej z której korzysta Zarządzający posiadający licencję, uwierzytelnienia MFA oraz bezpiecznych stacji w bezpiecznych lokalizacjach sieciowych;
2. w zależności od wyników analizy ryzyka przeprowadzanej przez Zarządzającego posiadającego licencję, mogą być stosowane inne mechanizmy zapewniające monitorowanie dostępu i rozliczalność działań dostawcy, np. przegląd logów lub nagrywanie sesji i jej parametrów w przypadku dostępu administracyjnego dostawcy lub dostępu personelu Zarządzającego posiadającego licencję o charakterze uprzywilejowanym.

SZABLONY

N/D

7. Dokumentowanie działań podmiotu nadzorowanego

TREŚĆ KOMUNIKATU UKNF

9. **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

1. Rozdział VII.9 Komunikatu określa wymogi organizacyjne i dokumentacyjne, które Zarządzający posiadający licencję wdrażający usługi chmury obliczeniowej powinien uwzględnić mając na uwadze potrzebę wykazania rozliczalności (np. w postaci wdrożonych polityk lub innych regulacji).
2. Dokumentowanie działań przez Zarządzającego posiadającego licencję jest procesem, który ma charakter ciągły. Zarządzający posiadający licencję powinien w szczególności uwzględnić potrzebę aktualizacji pozsiadanej dokumentacji wewnętrznej w trakcie korzystania z usług chmury obliczeniowej.
3. Zarządzający posiadający licencję, w zakresie w jakim to zasadne, przed rozpoczęciem korzystania z usług chmury obliczeniowej, powinien uwzględnić konieczność uzyskania stosownej dokumentacji od Dostawcy, w tym dostawcy usług chmury obliczeniowej.
    - *W ramach **Pośredniego stosowania Komunikatu**, Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego dotyczące dokumentowania działań Zarządzającego w zakresie przetwarzania informacji w usłudze chmury obliczeniowej i przekazywania określonych informacji oraz uzyskania stosownej dokumentacji od dostawcy usługi chmury obliczeniowej.*

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO POSIADAJĄCEGO LICENCJĘ

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, Zarządzający powinien udokumentować:
    1) schemat organizacji pracowników lub współpracowników Zarządzającego posiadającego licencję odpowiedzialnych za bezpieczeństwo, w tym cyberbezpieczeństwo, z uwzględnieniem elementów z pkt VII.9.1. a) Komunikatu;

2) architekturę sieci, systemów i aplikacji oraz punktów styku sieci wewnętrznych Zarządzającego posiadającego licencję z sieciami niezaufanymi, w tym architektury wdrażanego rozwiązania w chmurze obliczeniowej z uwzględnieniem środowisk testowych oraz scenariuszy awaryjnych;
3) zasady klasyfikacji informacji lub systemów pod kątem przetwarzania w chmurze obliczeniowej;
4) zasady stosowanych w organizacji zabezpieczeń technologicznych i rozwiązań organizacyjnych w odniesieniu do rozwiązań w chmurze obliczeniowej;
5) zasady (polityki) zarządzania ciągłością działania;
6) zasady bieżącego zabezpieczania przetwarzanych informacji dla wdrażanej usługi chmury obliczeniowej, jak również dla sytuacji planowanego lub nieplanowanego zakończenia współpracy z dostawcą usługi chmury obliczeniowej;
7) zasady (polityki) zarządzania zgodnością z prawem (m.in. procesy licencjonowania oprogramowania), w tym zgodnością z wymogami regulacyjnymi;
8) zasady (polityki) przeglądu i weryfikacji zarządczej systemu bezpieczeństwa związanego z korzystaniem z chmury obliczeniowej (np. coroczny przegląd);
9) zasady (polityki) raportowania, przeglądania i weryfikowania parametrów jakościowych funkcjonowania usług chmury obliczeniowej;
10) sformalizowaną umowę z dostawcą usługi chmury obliczeniowej wraz z dodatkowymi oświadczeniami, jeżeli to konieczne dla potwierdzenia spełnienia wymagań Komunikatu lub innego rodzaju wymagań, np. wynikających z powszechnie obowiązujących przepisów prawa;
11) opis procesów, procedury lub instrukcje, dotyczące obszarów wskazanych w podpunktach i. do vi. pkt VII.9.1.k) Komunikatu;
12) zasady zarządzania politykami i dokumentacją w ramach systemu zarządzania organizacją, zapewniające ochronę przed nieuprawnionym dostępem, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem.

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

N/D

SZABLONY

N/D

5. Zasady informowania UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w chmurze obliczeniowej

TREŚĆ KOMUNIKATU UKNF

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[12] 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

1. Z zastrzeżeniem pkt. 2 i 3 poniżej, Komunikat wymaga poinformowania UKNF o zamiarze przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej w zakresie jej części opartej o chmurę obliczeniową publiczną (w przypadku umowy zawieranej przez Zarządzającego posiadającego licencję z Dostawcą, w tym dostawcą usługi chmury obliczeniowej), gdy:
   1) usługi chmury obliczeniowej stanowią outsourcing szczególny chmury obliczeniowej lub
   2) w chmurze obliczeniowej przetwarzane są Informacje prawnie chronione.

   W przypadku współpracy dwóch Podmiotów nadzorowanych (np. w przypadku przetwarzania przez Zarządzającego posiadającego licencję w usłudze chmury obliczeniowej Informacji prawnie chronionych powierzonych przez TFI w związku z wykonywaniem umowy outsourcingowej

[12] Chyba że szczególny przepis prawa dotyczący działalności podmiotu nadzorowanego przewiduje inny termin przekazania informacji.

dotyczącej powierzenia Zarządzającemu posiadającemu licencje zarządzania sekurytyzowanymi wierzytelnościami funduszu sekurytyzacyjnego na podstawie zezwolenia, o którym mowa w art. 192 UFI) nie ma obowiązku dokonywania oddzielnych notyfikacji do UKNF uwzględniających korzystanie z chmury obliczeniowej przez obydwa te podmioty, jeśli korzystanie z chmury obliczeniowej jest autonomiczną decyzją jednego z Podmiotów nadzorowanych. W takim przypadku wystarczające jest dokonanie notyfikacji przez ten Podmiot nadzorowany, który podjął autonomiczną decyzję o korzystaniu z usług chmury obliczeniowej.

- *W ramach **Pośredniego stosowania Komunikatu** (np. gdy Zarządzający przetwarza w usłudze chmury obliczeniowej Informacje prawnie chronione powierzone przez Bank), notyfikacji dokonuje Powierzający podmiot nadzorowany (w w/w przypadku – Bank). W takim przypadku Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego co do wsparcia w uzupełnieniu formularza stanowiącego załącznik nr 1 do Komunikatu.*

2. Zgłoszenia należy dokonać co najmniej 14 dni przed rozpoczęciem przetwarzania informacji w chmurze obliczeniowej (niezależnie od samej daty zawarcia umowy)[13]. Oznacza to, że nie ma znaczenia samo zawarcie umowy z Dostawcą, ale istotna pozostaje data rozpoczęcia przetwarzania informacji przez Zarządzającego posiadającego licencję w chmurze obliczeniowej.
3. Uprawnionym do podpisania informacji, o której mowa rozdziale VIII. Komunikatu są osoby uprawnione do reprezentacji Zarządzającego posiadającego licencję (zgodnie z reprezentacją określoną w KRS), jak i osoby właściwie umocowane przez osoby uprawnione do reprezentacji.
4. W przypadku niespodziewanych okoliczności (sytuacji), które miałyby wpływ na stosowanie Komunikatu, Zarządzający posiadający licencję modyfikuje treść składanego oświadczenia zgodnie ze stanem faktycznym i informuje o tym UKNF odrębnym pismem z wyjaśnieniami.

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE ZARZĄDZAJĄCEGO POSIADAJĄCEGO LICENCJĘ

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

DZIAŁANIA DO PODJĘCIA / PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

N/D

SZABLONY

1. **Załącznik nr 7** do Standardu - Przykładowe wypełnienie informacji do UKNF o rozpoczęciu korzystania z chmury obliczeniowej przez Zarządzającego posiadającego licencję.

[13] Chyba że szczególny przepis prawa dotyczący działalności podmiotu nadzorowanego przewiduje inny termin przekazania informacji.

V. ZARZĄDZAJĄCY WIERZYTELNOŚCIAMI JAKO DOSTAWCA PODMIOTÓW NADZOROWANYCH – WYBRANE ZAGADNIENIA

1. Założenia rozdziału

Wzajemne powiązania podmiotów funkcjonujących na rynku finansowym i dynamicznie zmieniające się zależności między poszczególnymi branżami, czynią ten rynek wyjątkowo złożonym. Działania podmiotów Zarządzających wierzytelnościami są nieodzownym elementem zdrowego funkcjonowania nie tylko całego sektora, lecz także generalnie ekosystemu społeczno-gospodarczego, pozwalającym przywrócić do obiegu środki „zamrożone" – zaległe zobowiązania. Firmy zarządzające wierzytelnościami z uwagi na szeroką współpracę z innymi uczestnikami rynku finansowego powinny liczyć się z potrzebą respektowania nie tylko własnych obostrzeń regulacyjnych, lecz także uwarunkowań prawnych i nadzorczych dotyczących Podmiotów nadzorowanych, z którymi Zarządzający współpracują – w praktyce są to w szczególności TFI i Banki. Współpraca sektora bankowego z przedsiębiorstwami zarządzającymi wierzytelnościami przyczynia się przede wszystkim do poprawy płynności Banków. Z kolei w relacjach z TFI, Zarządzający działają głównie w roli Serwisera – jako podmiot zarządzający sekurytyzowanymi wierzytelnościami funduszu sekurytyzacyjnego w oparciu o udzielone przez organ nadzoru zezwolenie.

Z perspektywy Powierzających podmiotów nadzorowanych obie te relacje opierają się o umowę outsourcingową i determinują potrzebę spełnienia szeregu wymagań regulacyjnych wynikających w szczególności z Prawa bankowego oraz UFI. Ponadto w przypadku, w którym Zarządzający na potrzeby wykonania powierzonych czynności wykorzystuje chmurę obliczeniową, w sposób spełniający przesłanki stosowania Komunikatu, po stronie Powierzającego podmiotu nadzorowanego powstaje wynikający z rozdziału VI.2.7 Komunikatu obowiązek zapewnienia, że przetwarzanie informacji jest realizowane z uwzględnieniem jego postanowień. Weryfikacja spełnienia tych wymagań przez Powierzający podmiot nadzorowany obejmuje cały łańcuch outsourcingowy. Stąd też dalsze powierzenie czynności powierzonych Zarządzającemu do dostawcy usługi chmury obliczeniowej podlega nie tylko wymogom Komunikatu, lecz także przepisom prawa regulującym zasady dokonywania dalszego podpowierzenia. Zarządzający, który decyduje się na implementację technologii chmury obliczeniowej, współpracując z Powierzającymi podmiotami nadzorowanymi, powinien uwzględnić właściwe dla swoich Partnerów wymogi prawne i nadzorcze na możliwie najwcześniejszym etapie migracji.

2. Poniżej punktowo przedstawione zostaną wybrane, najistotniejsze zagadnienia wynikające z UFI, Prawa bankowego, UDUR i Rozporządzenia Delegowanego, z których koniecznością uwzględnienia albo oczekiwaniami Partnerów co do wykazania wypełnienia powinien liczyć się Zarządzający, który decyduje się na dalsze powierzenie czynności do dostawcy usługi chmury obliczeniowej. Należy mieć na uwadze, że przytoczone poniżej regulacje prawne nie stanowią pełnego

katalogu wymagań mających zastosowanie w przypadku outsourcingu we wskazanych sektorach regulowanych. Outsourcing TFI

Obszary istotne z perspektywy podoutsourcingu TFI

1. **Outsourcing w świetle przepisów art. 45a UFI**

a) **Rodzaje outsourcingu (art. 45a ust. 7 i 8 UFI).** Z uwagi na brzmienie przepisu art. 45a ust. 7 UFI, należy rozróżnić dwa możliwe rodzaje outsourcingu (podoutsourcingu) TFI, tj. outsourcing „niekwalifikowany" albo outsourcing „kwalifikowany":
   i. przez outsourcing „niekwalifikowany" należy rozumieć powierzenie przedsiębiorcy lub przedsiębiorcy zagranicznemu wykonywania czynności związanych z działalnością prowadzoną przez Towarzystwo – na podstawie umowy, 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 (art. 45a ust. 1 w zw. z art. 45a ust. 7 UFI);
   ii. zgodnie z art. 45a ust. 7 UFI *a contrario*, do kategorii outsourcingu „kwalifikowanego" należy zaliczyć kategorię umów, których przedmiotem są czynności mające istotne znaczenie 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.

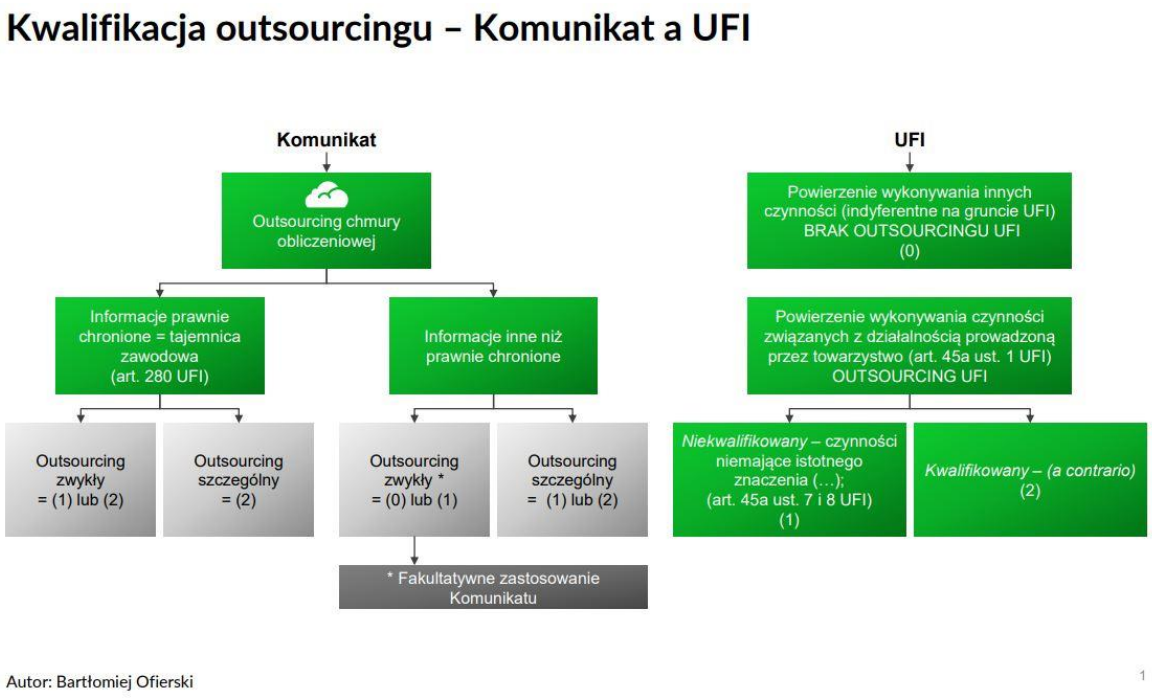
   Zakres wymogów zawartych w przepisach art. 45a dotyczących outsourcingu (podoutsourcingu) TFI, jest zróżnicowany w zależności od występującego rodzaju outsourcingu. Zgodnie bowiem z dyspozycją art. 45a ust. 7 UFI, w przypadku outsourcingu „niekwalifikowanego" nie stosuje się przepisów ust. 6, ust. 3 i 4 – w przypadku umów zawieranych przez Towarzystwo, ust. 4b i 4c – w przypadku przekazania lub dalszego przekazania wykonywania czynności związanych z działalnością prowadzoną przez Towarzystwo.
b) **Korelacja pomiędzy kwalifikacjami outsourcingu z UFI a Komunikatu.** Z perspektywy Towarzystwa jako Powierzającego podmiotu nadzorowanego istotne znaczenie ma odpowiednie zakwalifikowanie (według UFI) usług objętych podoutsourcingiem w sytuacji, gdy Zarządzający planuje dalsze powierzenie czynności do dostawcy usługi chmury obliczeniowej. Powinno się ono odbyć w korelacji z zakwalifikowaniem outsourcingu chmury obliczeniowej zgodnie właściwymi wytycznymi Komunikatu, tj. jako outsourcing chmury obliczeniowej szczególny albo inny niż szczególny. Ma to wpływ na zakres wymogów, do których stosowania będzie obowiązany Powierzający podmiot nadzorowany lub Zarządzający. Wzajemne powiązania dotyczące powyższych kwalifikacji zostały zobrazowane w poniższej grafice pt. „Kwalifikacja outsourcingu – UFI a Komunikat". Poszczególne, możliwe rodzaje outsourcingu chmury obliczeniowej w rozumieniu Komunikatu zostały przyporządkowane do danej kategorii kwalifikacji outsourcingu

z UFI, a kwalifikacja ta może obejmować na gruncie UFI trzy rodzaje ocen, według numeracji od (0) do (2), przy czym:

(0) – brak outsourcingu z UFI;

(1) – outsourcing „niekwalifikowany" z UFI;

(2) – outsourcing „kwalifikowany" z UFI.



c) **Zakres i nadzór nad podoutsourcingiem (art. 45a ust. 4 – 4d UFI).** Zarządzający planujący dalsze powierzenie czynności do dostawcy usługi chmury obliczeniowej powinien uwzględnić, w przypadku występowania outsourcingu „kwalifikowanego", konieczność uzyskania szczegółowej zgody Towarzystwa i uprzedniego poinformowania przez Towarzystwo Komisji o zamiarze takiego podpowierzenia.
W ramach relacji dalszego powierzenia w ramach outsourcingu „kwalifikowanego" muszą zostać również spełnione warunki wskazane w art. 45a ust. 4 UFI. Zarządzający powinien uwzględnić zatem ewentualne oczekiwania TFI w zakresie wsparcia w wykazaniu w szczególności, że:

i. podpowierzenie wykonywania czynności nie wpłynie niekorzystnie na sprawowanie przez KNF efektywnego nadzoru nad TFI oraz na interes uczestników funduszu;
ii. TFI posiada możliwość przekazywania poleceń podmiotom w ramach całego łańcucha outsourcingowego oraz nadzorowania wykonywanych podpowierzonych czynności oraz
iii. dostawca usługi chmurowej posiada odpowiednie kompetencje i sytuację finansową zapewniającą prawidłowe wykonanie umowy.

2. **Odpowiedzialność (art. 45a ust. 6 UFI).**

Przepisy prawa formalnie odnoszą się do zakresu odpowiedzialności TFI. Art. 45a ust. 6 UFI wprowadza zasadę solidarnej odpowiedzialności wobec uczestników funduszu TFI wraz z Zarządzającym, a w przypadku przekazania lub dalszego przekazania wykonywania czynności związanych z działalnością prowadzoną przez TFI innemu podmiotowi – również z tym podmiotem (zgodnie z art. 45a ust. 7 przepisu powyższego nie stosuje się w przypadku outsourcingu „niekwalifikowanego").

Z perspektywy skutków finansowych (zabezpieczenia interesów Zarządzającego) rekomendowane jest, aby Zarządzający w relacji z dostawcą usługi chmury obliczeniowej uwzględnił, w miarę możliwości, ewentualne własne zobowiązania względem TFI lub oczekiwania TFI dotyczące odpowiedzialności stron za szkody spowodowane niewykonaniem lub nienależytym wykonaniem umowy – tak, aby w przypadku niewykonania lub nienależytego wykonania umowy przez dostawcę usługi chmury obliczeniowej, możliwy był odpowiedni regres od dostawcy usługi chmury obliczeniowej.

3. **Łańcuch outsourcingowy (art. 45a ust. 4c – 4d UFI).**

Przepisy UFI nie określają limitu w zakresie dopuszczalnej długości łańcucha outsourcingowego TFI, na co wskazuje treść art. 45a ust. 4c i 4d UFI, które wskazują na możliwość dalszego podpowierzania czynności. Należy jednak mieć na uwadze (co dotyczy w szczególności outsourcingu „kwalifikowanego"), że dalsze powierzanie czynności wiąże się z koniecznością spełnienia określonych wymogów bez względu na miejsce poddostawcy w łańcuchu outsourcingowym (co wynika np. z art. 45a ust. 4b pkt. 2) w zw. z art. 45a ust. 4c).

4. **Kompetencje i ciągłość działania (art. 45 ust. 4 pkt. 5) UFI).**

Zarządzający powinien uwzględnić ewentualne oczekiwania TFI w zakresie wsparcia w wykazaniu, że dostawca usługi chmury obliczeniowej 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 (wymóg określony powyższym przepisem dotyczy outsourcingu „kwalifikowanego").

5. **Uprawnienia kontrolne Zarządzającego, Powierzającego podmiotu nadzorowanego i organu nadzoru (art. 45a ust. 4 UFI).**

Zarządzający w umowie z dostawcą usługi chmury obliczeniowej powinien uwzględnić potrzebę zapewnienia uprawnień kontrolnych względem dostawcy – zarówno Zarządzającemu jak i Powierzającemu podmiotowi nadzorowanemu oraz organowi nadzoru – co najmniej w zakresie oczekiwanym przez Powierzający podmiot nadzorowany.

6. **Tajemnica zawodowa (art. 280 UFI).**

a) Zarządzający w procesie outsourcingu chmury obliczeniowej powinien uwzględnić przepisy regulujące konieczność zachowania tajemnicy zawodowej, o której mowa w art. 280 ust. 1 UFI („**Tajemnica zawodowa**"), w ramach łańcucha outsourcingowego. Art. 280 UFI określa katalog podmiotów zobowiązanych do zachowania Tajemnicy zawodowej, są to m. in.: (i) osoby wchodzące w skład organów oraz pracownicy podmiotu, któremu na podstawie umowy zostało powierzone lub przekazane wykonywanie czynności towarzystwa oraz (ii) osoby pozostające z funduszem inwestycyjnym lub podmiotami, o których mowa w pkt. (i), w stosunku zlecenia lub innym stosunku prawnym o podobnym charakterze.
   Z treści przepisu można wywieść, że do zachowania Tajemnicy zawodowej zobowiązany jest dostawca TFI (Zarządzający) w związku z uzyskaniem informacji objętej Tajemnicą zawodową na podstawie umowy outsourcingowej, oraz odpowiednio – poddostawca (dostawca usługi chmury obliczeniowej). Ustawa nie określa zatem jasnej podstawy do dalszego ujawniania informacji prawnie chronionych. Niemniej – biorąc pod uwagę treść przepisów dotyczących łańcucha outsourcingowego, tj. art. 45a ust. 4c – 4d UFI oraz brak limitu w zakresie dopuszczalnej długości łańcucha outsourcingowego TFI (zob. pkt V.2.3) powyżej), oraz przy założeniu, że wykonywanie powierzonej czynności związanej z działalnością regulowaną może wiązać się z powierzeniem również informacji objętych Tajemnicą zawodową – zasadne jest zastosowanie wykładni funkcjonalnej. Wydaje się zatem, że brak limitu w zakresie dopuszczalnej długości łańcucha outsourcingowego TFI determinuje możliwość dalszego podpowierzania informacji, w tym informacji objętych Tajemnicą zawodową, w ramach całego łańcucha poddostawców.
   Na podstawie art. 280 ust. 2 UFI, można wskazać następujące przykłady informacji stanowiących Tajemnicę zawodową: informacje dotyczące nabywanych przez uczestników funduszu certyfikatów inwestycyjnych, dane osobowe osób zadłużonych wobec funduszu, informacje dotyczące charakterystyki nabytego przez fundusz portfela wierzytelności.
b) Obowiązek zachowania Tajemnicy zawodowej istnieje również po ustaniu umów zawartych w toku łańcucha outsourcingowego (art. 280 ust. 4 UFI). Wobec tego Zarządzający powinien uwzględnić oczekiwania Powierzającego podmiotu nadzorowanego co do zapewnienia, że Tajemnica zawodowa zostanie zachowana również po zakończeniu trwania ww. umów.

3. Outsourcing bankowy

Obszary istotne z perspektywy podoutsourcingu Banków

1. **Zakres i przesłanki podoutsourcingu (art. 6a ust. 7 Prawa bankowego).**

Zarządzający planujący dalsze powierzenie czynności do dostawcy usługi chmury obliczeniowej powinien uwzględnić konieczność:

i. posiadania generalnej zgody Banku na podoutsourcing zawartej w umowie outsourcingowej oraz
ii. uzyskania dodatkowej, pisemnej, szczegółowej zgody Banku na takie podpowierzenie. Zgoda powinna dotyczyć konkretnego dostawcy usługi chmury obliczeniowej oraz konkretnego zakresu powierzanych mu czynności.

Poddostawcy mogą być podpowierzone wyłącznie „czynności służące realizacji głównego świadczenia" wynikającego z umowy outsourcingu z Bankiem, przez które należy rozumieć czynności wspierające wykonywanie przedmiotu umowy przez Zarządzającego.

2. Uwzględnienie outsourcingu i podoutsourcingu w systemie zarządzania ryzykiem Banku (art. 6c Prawa bankowego).

Zarządzający powinien uwzględnić ewentualne oczekiwania Banku w zakresie:

i. wykazania, że podpowierzenie nie wpłynie niekorzystnie na prowadzenie przez Bank działalności zgodnie z przepisami prawa, ostrożne i stabilne zarządzanie bankiem, skuteczność systemu kontroli wewnętrznej w banku, możliwość wykonywania obowiązków przez biegłego rewidenta upoważnionego do badania sprawozdań finansowych banku na podstawie zawartej z bankiem umowy oraz ochronę tajemnicy prawnie chronionej;
ii. wsparcia Banku w analizie ryzyka związanego z podpowierzeniem czynności i uwzględnieniu tego ryzyka w systemie zarządzania ryzykiem Banku.

Ponadto Zarządzający jako dostawca Banku, na którym ciąży m. in. obowiązek posiadania planu ciągłości działania, powinien uwzględnić w tym planie ciągłości działania relację z dostawcą usługi chmurowej i zakres powierzanych mu czynności oraz nałożyć na dostawcę odpowiednie zobowiązania – co najmniej w zakresie, w jakim jest to niezbędne do wykonania planu ciągłości działania i z uwzględnieniem ewentualnych instrukcji Banku.

Oprócz wymagań w zakresie szacowania ryzyka związanego z korzystaniem przez Podmioty nadzorowane z usług przetwarzania danych w chmurze, wytyczne w zakresie sposobu dokonywania oceny dostawców IT oraz zarządzania ryzykiem związanym z korzystaniem przez Bank z usług dostawców IT ustanowione zostały m.in. w Rekomendacji M[14] oraz Rekomendacji D[15] Komisji Nadzoru Finansowego. Zgodnie z tą ostatnią, „procedury doboru usługodawców zewnętrznych – zwłaszcza w przypadku usług o istotnym znaczeniu dla banku – powinny uwzględniać ryzyko związane z danymi usługami i obejmować w szczególności ocenę sytuacji ekonomiczno-finansowej usługodawcy, zapewnianego przez niego poziomu bezpieczeństwa oraz jakości świadczonych usług (w miarę możliwości również na podstawie doświadczeń innych podmiotów)". Zarządzający powinien zatem uwzględnić ewentualne

[14] Rekomendacji M Komisji Nadzoru Finansowego dotyczącej zarządzania ryzykiem operacyjnym w bankach ze stycznia 2013 r.

[15] Rekomendacja D Komisji Nadzoru Finansowego dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach ze stycznia 2013 r.

oczekiwania Banku w zakresie weryfikacji wypełnienia wymogów ww. rekomendacji w ramach relacji outsourcingowej.

3. Wymogi dotyczące zarządzania poddostawcami oraz łańcucha outsourcingowego (art. 6a ust. 7, 6c ust. 3 Prawa bankowego).

Zarządzający powinien uwzględnić w umowie z dostawcą usługi chmury obliczeniowej zakaz dalszego podpowierzania czynności (zakaz dokonywania tzw. podoutsourcingu łańcuchowego, tj. wykraczającego poza zakres zezwolenia wynikającego z art. 6a ust. 7), z uwzględnieniem ewentualnych instrukcji Banku w tym zakresie. Łańcuch outsourcingowy powinien być ograniczony do jednego „poziomu" poddostawców, tj. poddostawcy bezpośredniego dostawcy Banku nie powinni korzystać z usług dalszych poddostawców. Zarządzający powinien uwzględnić także konieczność przekazania Bankowi szczegółowych informacji o poddostawcy (dostawcy usługi chmurowej), o których mowa w art. 6c ust. 3 Prawa bankowego.

Ponadto w kontekście tworzenia łańcucha outsourcingowego w rozdziale VI.2.7 Komunikatu wyrażone zostało stanowisko nadzoru w sprawie usług chmury obliczeniowej, które są wykorzystywane do świadczenia własnych usług przez bezpośrednich dostawców podmiotów nadzorowanych. Stanowisko to dotyczy m. in. sytuacji, w której bezpośredni Dostawca Banku (np. Zarządzający) korzysta z usługi chmurowej innego dostawcy (który na gruncie przepisów Prawa bankowego mógłby być uznany za poddostawcę, a na gruncie Komunikatu posiada status faktycznego dostawcy usług chmury obliczeniowej).

Zarządzający w związku z dalszym powierzeniem, powinien uwzględnić, że Bank na podstawie wymogów Komunikatu jest zobowiązany do dokonania weryfikacji, czy i w jakim zakresie jego bezpośredni dostawca wykorzystuje, w celu dostarczania usługi na rzecz Banku, usługę przetwarzania w chmurze. Ponadto Bank podlega pod wynikający z Komunikatu obowiązek zapewnienia zgodności wykorzystywania takiej usługi chmurowej z wymaganiami Komunikatu. Intencją organu nadzoru jest zatem objęcie zakresem stosowania Komunikatu korzystania z usług chmurowych niezależnie od tego, na jakim poziomie łańcucha outsourcingowego dochodzi do ich wykorzystania (z zastrzeżeniem, że liczba dopuszczalnych poziomów outsourcingu na gruncie Prawa bankowego jest ograniczona). Niezależnie zatem od tego, czy dostawca usług chmurowych jest bezpośrednim (w sensie formalnym) dostawcą Banku, Bank powinien przeprowadzić analizę wykorzystywanego rozwiązania, szacowanie ryzyka, weryfikację spełnienia minimalnych wymagań technicznych i organizacyjnych wynikających z Komunikatu itd. W analizowanym przypadku, w którym Zarządzający podpowierza czynności do dostawcy usługi chmurowej, Zarządzający powinien liczyć się z koniecznością spełnienia oczekiwań Banku co do wsparcia w wykazaniu ww. wymogów.

4. Tajemnica bankowa (art. 104 Prawa bankowego).

Zgodnie z przepisami Prawa bankowego regulującymi ochronę tajemnicy bankowej, Bank jest uprawniony do przekazania informacji objętych tą tajemnicą – w ramach outsourcingu – wyłącznie dostawcom oraz poddostawcom świadczącym usługi zgodnie z wymogami określonymi w przepisach art. 6a-6d Prawa bankowego oraz wyłącznie w niezbędnym

zakresie. Bank powinien zapewnić, że w związku z powierzeniem i podpowierzeniem czynności nie będzie dochodzić do ujawnienia Informacji prawnie chronionych na rzecz podmiotów nieuprawnionych na gruncie Prawa bankowego.

Zarządzający powinien zatem uwzględnić ograniczenia ciążące na Banku w zakresie możliwości ujawniania informacji w związku z powierzeniem czynności, w szczególności poprzez nałożenie odpowiednich obowiązków kontraktowych na dostawcę usługi chmury obliczeniowej oraz wdrożenie środków bezpieczeństwa – co najmniej w zakresie niezbędnym do realizacji zobowiązań Zarządzającego względem Banku. Ma to znaczenie w szczególności z uwagi na specyfikę sposobu funkcjonowania dostawców usług chmurowych, którzy modelowo angażują w świadczenie usług dalszych poddostawców.

Ponadto, zgodnie z Komunikatem, przez „ujawnienie informacji" należy rozumieć (bez uszczerbku dla rozumienia przepisów prawa bezwzględnie obowiązujących) sytuację, w której dochodzi do przetwarzania w chmurze obliczeniowej informacji:

i. w sposób nieszyfrowany albo
ii. 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.

W zakresie, w jakim jest to możliwe rekomendowanym działaniem jest:

i. stosowanie dostępnych zabezpieczeń technologicznych, w szczególności szyfrowanie informacji przetwarzanych w usługach dostawcy usługi chmury obliczeniowej kluczami Zarządzającego, do których dostępu nie będzie miał dostawca usługi chmury obliczeniowej ani żaden z jego ewentualnych poddostawców;
ii. korzystanie z funkcjonalności oferowanych przez dostawców usług chmury obliczeniowej pozwalających kontrolować udzielanie dostępów do danych.

5. Zakończenie współpracy (art. 6c ust. 5 Prawa bankowego).

Zarządzający powinien uwzględnić konieczność zapewnienia w umowie z dostawcą usługi chmurowej możliwości zmiany lub rozwiązania tej umowy (zaprzestania korzystania z usług dostawcy usługi chmury obliczeniowej w ramach realizowania czynności powierzonych Zarządzającemu przez Bank) zgodnie z instrukcjami Banku i w szczególności w związku z decyzją KNF, o której mowa w art. 6c ust. 5 Prawa bankowego. Zarządzający powinien uwzględnić ewentualną konieczność zaprzestania korzystania z usług dostawcy usługi chmury obliczeniowej w przetestowanym exit planie oraz planie ciągłości działania Zarządzającego.

6. Nieograniczona odpowiedzialność Zarządzającego (art. 6b Prawa bankowego).

Przepis Prawa bankowego zakazuje wyłączania odpowiedzialności Zarządzającego (jako Dostawcy) względem Banku za szkody wyrządzone klientom Banku wskutek niewykonania lub nienależytego wykonania umowy – dotyczy to zarówno umowy między Bankiem i

Zarządzającym jak i umowy Zarządzającego z poddostawcą (dostawcą usługi chmury obliczeniowej).

Natomiast z perspektywy skutków finansowych (zabezpieczenia interesów Zarządzającego jako Dostawcy) rekomendowane jest, aby Zarządzający w relacji z dostawcą usługi chmury obliczeniowej uwzględnił zakres własnych zobowiązań względem Banku, tak aby w przypadku niewykonania lub nienależytego wykonania umowy przez dostawcę usługi chmury obliczeniowej możliwy był odpowiedni regres od dostawcy usługi chmury obliczeniowej.

7. Uprawnienia kontrolne KNF (art. 6c ust. 4 i 5 Prawa bankowego).

Komisji Nadzoru Finansowego przysługuje szereg uprawnień nadzorczych i kontrolnych związanych z outsourcingiem, zarówno wobec Banku, jak i jego dostawców oraz poddostawców. Zarządzający jako Dostawca Banku powinien uwzględnić konieczność zapewnienia w umowie z poddostawcą (dostawcą usługi chmurowej) możliwości udostępnienia tej umowy Bankowi oraz KNF oraz przedstawienia wyjaśnień co do realizacji umowy – co najmniej każdorazowo na żądanie KNF.

Ponadto Zarządzający – co najmniej w zakresie określonym w umowie z Bankiem – powinien uwzględnić:

i. ewentualne oczekiwania Banku co do wsparcia w realizacji obowiązków Banku w zakresie współpracy z KNF wynikających z art. 6c ust. 4 i 5 Prawa bankowego oraz
ii. zakres uprawnień kontrolnych przysługujących KNF wobec dostawców oraz poddostawców Banku zgodnie z art. 6c ust. 8 Prawa bankowego.

Zgodnie z właściwymi przepisami Prawa bankowego, dostawcy oraz poddostawcy powinni zatem m.in. umożliwić inspektorom nadzoru bankowego oraz osobom upoważnionym przez KNF przeprowadzenie czynności kontrolnych oraz umożliwić upoważnionym osobom wykonywanie czynności określonych w art. 133 ust. 2 Prawa bankowego, a w szczególności udostępnić do wglądu księgi, bilanse, rejestry, plany, sprawozdania i inne dokumenty oraz umożliwić, na pisemne żądanie, sporządzenie kopii tych dokumentów i innych nośników informacji, jak również udzielać wyjaśnień żądanych przez te osoby. W umowie z poddostawcą (dostawcą usług chmurowych) Zarządzający powinien zatem zapewnić sobie uprawnienia pozwalające na wykonanie zobowiązań Zarządzającego wynikających z umowy z Bankiem, w szczególności poprzez określenie odpowiednich obowiązków kontraktowych dostawcy usługi chmury obliczeniowej w tym zakresie.

8. Podoutsourcing zagraniczny (art. 6d Prawa bankowego).

Zarządzający w procesie wyboru dostawcy usługi chmury obliczeniowej powinien uwzględnić konsekwencje wejścia w reżim outsourcingu zagranicznego. W szczególności Zarządzający powinien uwzględnić stanowisko Banku co do możliwości podpowierzenia czynności przedsiębiorcy zagranicznemu, a w przypadku zgody Banku na takie podpowierzenie – uwzględnić konieczność uzyskania zezwolenia Komisji Nadzoru Finansowego na outsourcing zagraniczny udzielanego na wniosek Banku. Uzyskanie zezwolenia KNF będzie wymagane w

przypadku zamiaru zawarcia umowy z dostawcą posiadającym siedzibę lub świadczącym usługę poza EOG (np. przetwarzającym informacje Banku w centrum przetwarzania danych znajdującym się poza EOG). W praktyce oznacza to przede wszystkim konieczność ustanowienia w umowie z dostawcą usług chmurowych zasad zapewniających Zarządzającemu ścisłą kontrolę nad lokalizacją świadczenia usług (np. zapewnienia dotyczące korzystania z centrów przetwarzania danych znajdujących się wyłącznie na terytorium państw należących do EOG).

4. Outsourcing ubezpieczeniowy

Obszary istotne z perspektywy podoutsourcingu Zakładów Ubezpieczeń

1. **Tajemnica ubezpieczeniowa (art. 35 ust. 1 UDUR, art. 274 ust. 4 lit. g) Rozporządzenia Delegowanego).**

a) Zarządzający w procesie outsourcingu chmury obliczeniowej powinien uwzględnić konieczność ochrony informacji objętych tajemnicą ubezpieczeniową, o której mowa w art. 35 ust. 1 UDUR. Obowiązek zachowania tajemnicy dotyczącej poszczególnych umów ubezpieczenia spoczywa m. in. na osobach i podmiotach, za pomocą których ZU wykonuje czynności ubezpieczeniowe. Ponadto obowiązek ochrony przez Zarządzającego jako dostawcy ZU wszystkich informacji poufnych dotyczących Zakładu Ubezpieczeń oraz jego ubezpieczających, beneficjentów, pracowników, kontrahentów i wszelkich innych osób wynika z Rozporządzenie Delegowanego.
b) Przepisy sektorowe regulujące outsourcing ZU nie dają jednoznacznej podstawy dla ujawnienia informacji objętych tajemnicą ubezpieczeniową, o której mowa w art. 35 ust. 1 UDUR na rzecz poddostawców wykorzystywanych przez Zarządzających świadczących usługi na rzecz ZU.

2. **Współpraca z organem nadzoru i uprawnienia audytowe (art. 74 UDUR i art. 274 ust. 4. lit. h) Rozporządzenia Delegowanego).**

a) Podejmując współpracę z ZU, Zarządzający powinien uwzględnić wynikające z wymogów sektorowych możliwe oczekiwanie ZU co do współpracy jego dostawcy (Zarządzającego) z organem nadzoru oraz zapewnienia możliwości realizacji uprawnień audytowych przysługujących ZU, jego audytorom zewnętrznym oraz organowi nadzoru – względem Zarządzającego jako dostawcy ZU.
   Zgodnie z art. 74 UDUR outsourcing czynności ubezpieczeniowych lub reasekuracyjnych oraz funkcji należących do systemu zarządzania może odbywać się wyłącznie pod warunkiem, że Zarządzający w zakresie powierzonych czynności lub funkcji:
   i. będzie współpracował z organem nadzoru,
   ii. zapewni organowi nadzoru możliwość przeprowadzenia kontroli swojej działalności i stanu majątkowego.

   Ponadto ZU, firma audytorska badająca sprawozdania finansowe ZU, firma audytorska badająca sprawozdania o wypłacalności i kondycji finansowej ZU oraz

organ nadzoru powinny posiadać dostęp do danych związanych z powierzonymi czynnościami lub funkcjami.

b) Uwzględniając wymóg art. 274 ust. 4 lit. h) i i) Rozporządzenia Delegowanego, Zarządzający powinien liczyć się z oczekiwaniami ZU co do zapewnienia w umowie outsourcingu bardziej szczegółowych uprawnień kontrolnych, w tym zagwarantowania:
   i. ZU, audytorom zewnętrznym oraz organowi nadzoru:
      a. faktycznego dostępu do wszystkich informacji dotyczących funkcji i czynności zlecanych w drodze outsourcingu, a także
      b. możliwości prowadzenia kontroli na miejscu, w lokalu Zarządzającego;
   ii. organowi nadzoru:
      a. możliwości kierowania zapytań bezpośrednio do Zarządzającego, gdy jest to stosowne i konieczne do celów nadzorczych, oraz
      b. obowiązku udzielenia przez Zarządzającego odpowiedzi na te pytania.

c) Zważywszy, że ZU może oczekiwać zapewnienia uprawnień audytowych także względem poddostawców Zarządzającego, Zarządzający powinien uwzględnić potrzebę uzyskania odpowiednich zapewnień ze strony bezpośredniego dostawcy ZU – zarówno w aspekcie podmiotowym (dla ww. podmiotów), jak i przedmiotowym (co najmniej w zakresie określonym w przepisach sektorowych).

3. Zawiadomienie KNF (art. 75 ust. 2 UDUR).

Zgodnie z art. 75 ust. 2 UDUR, ZU powinien zawiadomić KNF co najmniej na 30 dni przed wdrożeniem outsourcingu, jeśli powierzone funkcje ZU zaliczy do należących do systemu zarządzania lub podstawowych lub ważnych czynności, a także o każdej istotnej zmianie w outsourcingu tych funkcji lub czynności. Jednocześnie jednak, zgodnie z pkt. VIII.1. Komunikatu chmurowego UKNF, ZU powinien poinformować KNF o zamiarze przetwarzania danych w chmurze obliczeniowej w terminie 14 dni przed jego rozpoczęciem.

Niemniej, zgodnie z Komunikatem chmurowym UKNF termin zawiadomienia KNF może różnić się od określonego w Komunikacie, jeśli wynika to ze szczególnego przepisu prawa dotyczącego działalności podmiotu nadzorowanego. Przypadek taki stanowi regulacja zawarta w UDUR: wydłużony, 30-dniowy termin notyfikacji znajdzie zastosowanie wówczas, gdy outsourcing, którego dotyczyć ma zawiadomienie, spełnia wymagania określone w art. 75 ust. 2 UDUR. W pozostałych przypadkach (spełniających kryteria outsourcingu podlegającego notyfikacji zgodnie z Komunikatem chmurowym UKNF, ale nie wchodzących jednocześnie w zakres regulacji art. 75 ust.2 UDUR) za właściwy uznać należy termin 14 dni.

4. Nieograniczona odpowiedzialność ZU (art. 76 UDUR).

a) Zgodnie z UDUR odpowiedzialności ZU za szkody wyrządzone ubezpieczającym, ubezpieczonym uprawnionym z umów ubezpieczenia lub cedentom wskutek niewykonania lub nienależytego wykonania outsourcingu nie można wyłączyć ani ograniczyć.

b) Wymóg ten nie wprowadza ograniczeń co do zakresu odpowiedzialności Zarządzającego jako dostawcy ZU – odpowiedzialność ta może więc podlegać ograniczeniom lub zostać wyłączona. Niemniej jednak, należy mieć na uwadze stanowisko nadzoru, w ramach którego nadzór wyraża krytyczną ocenę wobec wyłączeń lub ograniczeń odpowiedzialności dostawców usług chmury obliczeniowej wobec ZU, 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.

5. Podoutsourcing (art. 274 ust. 4 lit. k) i l) Rozporządzenia Delegowanego).

a) Zarządzający korzystający z usług poddostawców, w tym świadczących usługi chmury obliczeniowej, powinien brać pod uwagę konieczność zaakceptowania w umowie z ZU oraz odpowiednio uwzględnienia w umowach zawieranych z poddostawcami, postanowień określających warunki, zgodnie z którymi Zarządzający może dokonać podoutsourcingu funkcji i czynności zleconych mu w drodze outsourcingu (art. 274 ust. 4 lit. k) Rozporządzenia Delegowanego). W tym zakresie ZU może oczekiwać od Zarządzającego w szczególności umownego wskazania:
    i. poddostawców, z usług których Zarządzający korzysta w chwili zawarcia umowy outsourcingu;
    ii. sposobu angażowania nowych poddostawców;
    iii. prawa sprzeciwu ZU wobec zaangażowania określonego poddostawcy w proces świadczenia usług;
    iv. zakresu i sposobu nadawania poddostawcom dostępu do informacji powierzonych przez ZU;
    v. lokalizacji świadczenia usług przez poddostawców.
b) Ponadto zgodnie z art. 274 ust. 4 lit. l) Rozporządzenia Delegowanego umowa outsourcingu zawierana pomiędzy ZU a Zarządzającym powinna zawierać zobowiązanie Zarządzającego, zgodnie z którym wynikające z tej umowy obowiązki i zadania Zarządzającego pozostaną nienaruszone pomimo ewentualnego podoutsourcingu.

6. Obowiązek utrzymywania planów awaryjnych (art. 274 ust. 5 lit. d) Rozporządzenia Delegowanego).

W przypadkach, w których w drodze outsourcingu zlecane są podstawowe lub ważne funkcje lub czynności operacyjne, Zarządzający działający jako dostawca ZU, powinien uwzględnić konieczność utrzymywania planów awaryjnych. Plany te powinny zostać odpowiednio opracowane przez Zarządzającego na wypadek wystąpienia sytuacji nadzwyczajnych lub zakłócenia działalności gospodarczej. Art. 274 ust. 5 lit. d) Rozporządzenia Delegowanego przewiduje przy tym obowiązek zapewnienia, że Zarządzający będzie – w razie konieczności

– okresowo testować infrastrukturę rezerwową, uwzględniając funkcje i czynności zlecone w drodze outsourcingu.

Zarządzający powinien mieć na uwadze, że ZU może oczekiwać odzwierciedlenia powyższych obowiązków w umowach zawieranych z poddostawcami Zarządzającego, w tym – dostawcą usługi chmury obliczeniowej.

7. Inne wymogi dla umów outsourcingu (art. 274 ust. 4 Rozporządzenia Delegowanego).

Poza wymogami opisanymi w punktach powyżej, Zarządzający działający jako dostawca ZU powinien liczyć się z koniecznością zapewnienia w umowie outsourcingu zawieranej z ZU także innych wymogów kontraktowych wynikających z treści art. 274 ust. 4 Rozporządzenia Delegowanego. Zgodnie z tym przepisem w pisemnej umowie outsourcingu należy wyraźnie sformułować:

i. obowiązki i zadania obu stron (art. 274 ust. 4 lit. a) Rozporządzenia Delegowanego);
ii. zobowiązanie Zarządzającego do przestrzegania wszystkich mających zastosowanie przepisów prawa, wymogów regulacyjnych i wytycznych, jak również wszelkich zasad zatwierdzonych przez ZU (art. 274 ust. 4 lit. b) Rozporządzenia Delegowanego);
iii. zobowiązanie Zarządzającego do ujawniania wszelkich faktów mogących w istotny sposób wpłynąć na jego zdolność do wykonania zleconych mu w drodze outsourcingu funkcji lub czynności w sposób skuteczny i zgodny z odpowiednimi przepisami prawa i wymogami regulacyjnymi (art. 274 ust. 4 lit. c) Rozporządzenia Delegowanego);
iv. zastrzeżone przez ZU prawo do bycia informowanym przez Zarządzającego o funkcjach i czynnościach zleconych w drodze outsourcingu oraz o ich realizacji, a także prawo do wydawania ogólnych wytycznych i indywidualnych instrukcji skierowanych do Zarządzającego w sprawie kwestii, które należy uwzględnić podczas wykonywania funkcji i czynności zleconych w drodze outsourcingu (art. 274 ust. 4 lit. f) Rozporządzenia Delegowanego);
v. prawo ZU do otrzymania informacji o funkcjach i czynnościach zleconych w drodze outsourcingu oraz możliwość wydawania instrukcji w sprawie funkcji i czynności zleconych w drodze outsourcingu (art. 274 ust. 4 lit. j) Rozporządzenia Delegowanego).

Załączniki:

1. Modelowe wdrożenie usługi przetwarzania informacji w chmurze obliczeniowej publicznej. lub hybrydowej dla Zarządzających wierzytelnościami.
2. Wzorcowa dokumentacja klasyfikacji i oceny informacji.
3. Przykład szablonu szacowania ryzyka.
4. Założenia metodyki w zakresie przetwarzania informacji w chmurze obliczeniowej zgodnie z Komunikatem chmurowym UKNF.
5. Wzorcowy plan przetwarzania informacji w chmurze obliczeniowej.
6. Wzorcowy szablon scenariusza wyjścia z chmury.
7. Przykładowe wypełnienie informacji do UKNF o rozpoczęciu korzystania z chmury obliczeniowej przez Zarządzającego posiadającego licencję.
8. Analiza ISO 27001.
9. Wytyczne do opracowania planu ciągłości działania.
10. Pytania skierowane przez ZPF w związku z przygotowaniem Standardu i odpowiedzi UKNF.

Załącznik 1. Modelowe wdrożenie usługi przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej dla Zarządzających wierzytelnościami

1. WSTĘP

Niniejszy dokument opisuje przykładowe kroki wdrożenia usługi przetwarzania informacji w chmurze obliczeniowej w ramach Bezpośredniego stosowania Komunikatu. Ponadto w dokumencie uwzględnione zostały punktowe wskazówki co do modelu wdrożenia w ramach Pośredniego stosowania Komunikatu.

Opisane poniżej kroki mogą być stosowane dla realizacji procesu chmurowego z uwzględnieniem specyfiki Modelu usługi chmury obliczeniowej w ramach odpowiednio Bezpośredniego stosowania Komunikatu oraz oczekiwań Powierzającego podmiotu nadzorowanego w ramach Pośredniego stosowania Komunikatu. Kroki, których realizację przewiduje Komunikat chmurowy UKNF oznaczono na fioletowo.

Zidentyfikowanie potrzeby biznesowej

1. Identyfikacja i udokumentowanie potrzeby biznesowej, zgodnie z procedurami obowiązującymi Zarządzającego posiadającego licencję.

2. Otwarcie projektu, uruchomienie procesu zarządzania zmianą lub innej inicjatywy, która pozwala na przypisanie prac i zadań związanych z dalszymi działaniami.

3. Określenie zasadności dalszej analizy potrzeby biznesowej przez jednostki odpowiedzialne za architekturę, technologię oraz bezpieczeństwo pod kątem możliwości wdrożenia usługi przetwarzania informacji w chmurze obliczeniowej.

Produkty

1. Udokumentowana potrzeba biznesowa z opisem wymagań.

2. Wniosek lub zgłoszenie otwierające projekt, zmianę lub inną inicjatywę.

2. WSTĘPNA OCENA MOŻLIWOŚCI REALIZACJI POTRZEBY BIZNESOWEJ

1. Wstępna ocena możliwości realizacji potrzeby biznesowej w usłudze chmurze obliczeniowej, tj.:
   a. analiza i porównanie rozwiązań w usłudze chmury obliczeniowej vs. *on-premise* – wstępna ocena realizacji wymagań i kosztów; analiza potencjalnych dostawców usług chmury obliczeniowej;
   b. architektura, integracja, docelowa konfiguracja – zgodność z docelową architekturą Zarządzającego posiadającego licencję;
   c. wstępne PoC rozwiązania, jeśli planowane jest wykorzystanie całkowicie nowych dla Zarządzającego technologii;
   d. wstępna inwentaryzacja i klasyfikacja informacji Zarządzającego posiadającego licencję;

e. klasyfikacja istotności usługi chmury obliczeniowej dla Zarządzającego posiadającego licencję – w zależności od wyników podejmowana jest wstępna decyzja pod kątem stosowania Komunikatu;
f. zbadanie możliwości pozyskania kompetencji dla usługi chmury obliczeniowej i on-premise;
g. zgodność ze strategią Zarządzającego posiadającego licencję;
h. zgodność z regulacjami wewnętrznymi Zarządzającego posiadającego licencję.

- *W ramach **Pośredniego stosowania Komunikatu** Zarządzający określa planowany zakres przetwarzania informacji w chmurze obliczeniowej, w szczególności określa kategorie informacji/ rodzaje czynności lub funkcji powierzonych Zarządzającemu przez Powierzający podmiot nadzorowany, których przetwarzanie lub realizacja w usłudze chmury obliczeniowej może determinować obowiązek stosowania Komunikatu przez Powierzający podmiot nadzorowany.*
- *W przypadku, w którym w/w identyfikacja wskazuje na obowiązek stosowania Komunikatu przez Powierzający podmiot nadzorowany w związku z korzystaniem z usług chmury obliczeniowej przez Zarządzającego, Zarządzający weryfikuje podstawy i ewentualne ograniczenia kontraktowe w ramach umów z Powierzającym podmiotem nadzorowanym co do możliwości wykorzystywania chmury obliczeniowej na potrzeby wykonywania czynności przetwarzania zleconych przez Powierzający podmiot nadzorowany.*
- *W przypadku, w którym w/w weryfikacja nie pozwala na jednoznaczną ocenę możliwości wykorzystywania chmury obliczeniowej na potrzeby wykonywania czynności przetwarzania zleconych przez Powierzający podmiot nadzorowany, Zarządzający konsultuje z Powierzającym podmiotem nadzorowanym taką możliwość i w miarę możliwości określa zasady dalszego powierzenia.*

Produkty

1. Wstępna analiza wykonalności pod kątem usługi chmury obliczeniowej vs. on-premise.

   *W ramach **Pośredniego stosowania Komunikatu**: wstępna analiza możliwości wykonywania czynności przetwarzania zleconych przez Powierzający podmiot nadzorowany w usłudze chmury obliczeniowej.*

3. DECYZJA O DOPUSZCZALNOŚCI WDROŻENIA USŁUGI CHMURY OBLICZENIOWEJ

1. Decyzja o dalszym procesowaniu potrzeby biznesowej, która zakłada poniższe scenariusze:

   a. Scenariusz 1.: brak możliwości lub uzasadnienia do wykorzystania usługi chmury obliczeniowej;
   b. Scenariusz 2.: dopuszczalne wdrożenie usługi chmury obliczeniowej – z zastrzeżeniem konieczności Bezpośredniego stosowania Komunikatu lub Pośredniego stosowania Komunikatu;
   c. Scenariusz 3.: dopuszczalne wdrożenie usługi chmury obliczeniowej – w przypadku, gdy Komunikat nie ma zastosowania lub Zarządzający posiadający licencję nie zidentyfikował potrzeby zarówno Bezpośredniego stosowania Komunikatu, jak i Pośredniego stosowania Komunikatu.

2. Dalsze kroki będą opisywane tylko dla Scenariusza 2.

Produkty

1. Udokumentowana decyzja o możliwości wdrożenia usługi chmury obliczeniowej (osoby umocowane zgodnie z regulacjami wewnętrznymi Zarządzającego posiadającego licencję).

4. OPRACOWANIE WYMAGAŃ DO WDROŻENIA USŁUGI CHMURY OBLICZENIOWEJ

1. Określenie katalogu wymagań biznesowych, formalnoprawnych, bezpieczeństwa lub innych, w szczególności wynikających z wymogów regulacyjnych i nadzorczych dotyczących Zarządzającego posiadającego licencję oraz regulacji wewnętrznych Zarządzającego posiadającego licencję w związku z realizacją potrzeby biznesowej w usłudze chmurze obliczeniowej.

2. Określając wymagania, rekomendowane jest uwzględnienie poniższych kwestii:
   a. Czy istnieją na rynku usługi chmury obliczeniowej posiadające referencje w branży finansowej?
   b. Czy potencjalni oferenci mogą zapewnić CPD na terenie EOG?
   c. Czy możliwe jest zapewnienie odpowiednich kompetencji po stronie Zarządzającego posiadającego licencję? Czy są wymagane dodatkowe szkolenia dla pracowników? Jakie są możliwości na rynku? Z jakimi kosztami należy się liczyć?
   d. Czy dostawca usług chmury obliczeniowej potwierdza zgodność przetwarzania danych osobowych zgodnie z regulacjami wewnętrznymi Zarządzającego posiadającego licencję i powszechnie obowiązującymi przepisami prawa oraz Komunikatem?
   e. Czy chmura obliczeniowa będzie w stanie zapewnić wymaganą pojemność i wydajność?
   f. Zasady przekazywania informacji odnośnie do zdarzeń naruszenia bezpieczeństwa informacji, rozumianego jako poufność, integralność i dostępność przetwarzanych informacji i zasobów, ze szczególnym uwzględnieniem Informacji prawnie chronionych.
   g. Zasady zakończenia współpracy z dostawcą usług chmury obliczeniowej, w tym zasady bezpiecznego i trwałego usuwania informacji z usługi chmury obliczeniowej.
   h. Monitorowanie parametrów działania usług chmury obliczeniowej, z których miałby korzystać Zarządzający posiadający licencję.
   i. Wykonywanie zobowiązań wynikających z umowy, w ustalonym zakresie i terminie, z zachowaniem należytej staranności, z uwzględnieniem zawodowego charakteru prowadzonej działalności gospodarczej.
   - *W ramach **Pośredniego stosowania Komunikatu** Zarządzający, określając katalog wymagań w miarę możliwości uwzględnia dodatkowo ewentualne oczekiwania Powierzającego podmiotu nadzorowanego (w szczególności zdeterminowane obowiązkami regulacyjnymi Powierzającego podmiotu nadzorowanego).*

3. Wymagania wynikające z Komunikatu względem dostawcy usług chmury obliczeniowej zostały wskazane w sekcji działania do podjęcia / produkty do opracowania po stronie dostawcy usług chmury obliczeniowej do każdej z omawianych w Standardzie części Komunikatu.

Produkty

1. Udokumentowane wymagania do usługi chmury obliczeniowej.

5. ANALIZA OFERT I WSTĘPNA ANALIZA RYZYKA

1. Opracowanie i przekazanie dokumentu zapytania ofertowego do dostawców usług chmury obliczeniowej. Zapytanie ofertowe powinno w miarę możliwości uwzględniać wymagania wskazane w pkt. 5 powyżej, w tym wskazane w sekcji działania do podjęcia / produkty do opracowania po stronie dostawcy usług chmury obliczeniowej do każdej z omawianych w Standardzie części Komunikatu.

2. Przeprowadzenie wstępnej analiza ryzyka dla oferowanych usług chmury obliczeniowej na podstawie odpowiedzi dostawców usług chmury obliczeniowej z uwzględnieniem stopnia spełnienia wymagań wskazanych w pkt. 4 powyżej. Wymagania wskazane w sekcji działania do podjęcia / produkty do opracowania po stronie dostawcy usług chmury obliczeniowej do każdej z omawianych w Standardzie części Komunikatu stanowią minimalne wymagania, których spełnienie powinno być wymagane do wdrożenia usługi chmury obliczeniowej. Dla pozostałych wymagań, możliwe jest zaproponowanie rozwiązań tymczasowych lub mechanizmów kontrolnych zapewniających akceptowalny poziom ryzyka.

3. Oferty, które nie spełniają w/w minimalnych wymagań, powinny zostać odrzucone.

4. Wynik wstępnej analizy ryzyka, łącznie z wymaganiami funkcjonalnymi, aspektami finansowymi etc., jest podstawą do podjęcia decyzji o wyborze dostawcy usług chmury obliczeniowej dla danej potrzeby biznesowej.
    - *W ramach **Pośredniego stosowania Komunikatu** Zarządzający w procesie wyboru dostawcy oraz oceny ryzyka w miarę możliwości uwzględnia ewentualne wymagania Powierzającego podmiotu nadzorowanego (w szczególności zdeterminowane obowiązkami regulacyjnymi Powierzającego podmiotu nadzorowanego) m. in. co do umowy z dostawcą usługi chmurowej, zasad bezpieczeństwa i aspektów technologicznych.*

Produkty

1. Zapytanie ofertowe i odpowiedzi na zapytanie.

2. Weryfikacja spełnienia wymagań wskazanych w pkt. 4 powyżej.

3. Wstępna analiza ryzyka dla ofert, które nie zostały odrzucone wraz z proponowanym planem postępowania z ewentualnie zidentyfikowanymi ryzykami.

6. WYBÓR DOSTAWCY. ANALIZA RYZYKA

1. Wybór oferty.

2. Finalna, kompleksowa identyfikacja i analiza ryzyka dla wybranej oferty w obszarach (i) prawnym – w tym szczegółowa formalnoprawna analiza umowy, (ii) technologicznym i (iii) organizacyjnym poprzedzona etapem klasyfikacji i oceny informacji przetwarzanych w chmurze obliczeniowej zgodnie z wymogami Komunikatu.

3. Określenie (jeśli to zasadne – wspólnie z dostawcą usług chmury obliczeniowej) środków zaradczych do zastosowania względem zidentyfikowanych zagrożeń i opracowanie planu postępowania z ryzykiem.
    - *W ramach **Pośredniego stosowania Komunikatu** Zarządzający w procesie analizy ryzyka w miarę możliwości uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego (w szczególności zdeterminowane obowiązkami regulacyjnymi Powierzającego podmiotu nadzorowanego) m. in. co do umowy z dostawcą usług chmurowych, zasad bezpieczeństwa i aspektów technologicznych.*

Produkty

1. Wybór oferty wraz z uzasadnieniem.

2. Dokument analizy ryzyka dla wybranej oferty.

3. Plan postępowania z ryzykiem.

7. PODPISANIE UMOWY

1. Zaadresowanie ewentualnych zidentyfikowanych w ramach pkt. 6 powyżej ryzyk poprzez wprowadzenie do projektu umowy z dostawcą usługi chmury obliczeniowej postanowień, planów naprawczych, etc., mających na celu mitygację tych ryzyk.

2. Podpisanie umowy z dostawcą usługi chmury obliczeniowej.

Produkty

1. **Podpisana umowa.** Zalecane jest, aby decyzja o migracji chmurowej była poprzedzona udokumentowaną zgodą Zarządu Zarządzającego posiadającego licencję.

2. Aktualizacja statusu planu postępowania ze zidentyfikowanymi rodzajami ryzyka.

8. WDROŻENIE PRZEDPRODUKCYJNE – KONFIGURACJA USŁUGI

1. **Realizacja kluczowych kamieni milowych wynikających z Komunikatu, w tym w szczególności:**

    a. **opracowanie dokumentacji usługi chmury obliczeniowej, w szczególności klasyfikacji i oceny informacji oraz szacowania ryzyka;**
    b. dostosowanie procedur wewnętrznych Zarządzającego posiadającego licencję;
    c. **pozyskanie kompetencji;**
    d. **opracowanie planu przetwarzania informacji w chmurze obliczeniowej;**
    e. **opracowanie planu wyjścia;**
    f. **opracowanie planu ciągłości działania (BCP) lub modyfikacja istniejącego;**
    g. **wdrożenie zabezpieczeń i mechanizmów monitorowania (np. integracja ze SIEM, etc.);**
    h. **testy (funkcjonalne, akceptacyjne, bezpieczeństwa, wydajnościowe, etc.)**

2. Na etapie wdrożenia przedprodukcyjnego (konfiguracji usług) nie jest jeszcze dokonywana migracja danych produkcyjnych.

3. Po zakończeniu wdrożenia – aktualizacja statusu planów naprawczych i **dokumentacji szacowania ryzyka w celu potwierdzenia, że zidentyfikowane ryzyka zostały zaadresowane zgodnie z założeniami.**

4. Określenie planu migracji i uruchomienia produkcyjnego.

Produkty

1. **Dokumentacja usługi chmury obliczeniowej (w tym klasyfikacja i ocena informacji i szacowanie ryzyka).**

2. Dostosowane procedury wewnętrzne Zarządzającego posiadającego licencję.

3. **Dokumentacja szkoleń / pozyskania kompetencji dla użytkowników końcowych i innych kluczowych ról.**

4. **Plan przetwarzania informacji w chmurze obliczeniowej.**

5. **Plan wyjścia z usługi chmury obliczeniowej.**

6. **Plan ciągłości działania.**

7. **Dokumentacja wdrożenia zabezpieczeń mechanizmów kontrolnych, plan postępowania z ryzykiem.**

8. **Wyniki testów i ich akceptacja.**

9. Plan migracji i wdrożenia produkcyjnego.
    - *W ramach **Pośredniego stosowania Komunikatu** Zarządzający uwzględnia ewentualne wymagania Powierzającego podmiotu nadzorowanego (w szczególności zdeterminowane obowiązkami regulacyjnymi Powierzającego podmiotu nadzorowanego) co do wdrożenia usługi chmury obliczeniowej, w szczególności w zakresie stosowanych standardów bezpieczeństwa i środków zaradczych względem zidentyfikowanych ryzyk oraz dokumentacji / informacji, których przekazania oczekuje Powierzający podmiot nadzorowany.*

9. INFORMOWANIE UKNF

1. **Uzupełnienie i przekazanie UKNF zgodnie z wymaganiami Komunikatu dokumentu „Informacja podmiotu nadzorowanego w sprawie przetwarzania informacji w chmurze obliczeniowej" stanowiącego Załącznik nr 1 do Komunikatu.**

Produkty

1. **Uzupełniony formularz stanowiący Załącznik nr 1 do Komunikatu, dostarczony do UKNF.**
    - ***Zarządzający posiadający licencję, w zakresie w jakim jest równocześnie zobowiązany do Bezpośredniego stosowania Komunikatu jak i Pośredniego stosowania Komunikatu (np. w przypadku przetwarzania przez Zarządzającego posiadającego licencję w usłudze chmury obliczeniowej Informacji prawnie chronionych powierzonych przez TFI w związku z wykonywaniem umowy outsourcingowej dotyczącej powierzeniu Zarządzającemu posiadającemu licencję zarządzania sekurytyzowanymi wierzytelnościami funduszu sekurytyzacyjnego na podstawie zezwolenia, o którym mowa w art. 192 UFI), uwzględnia wymóg samodzielnej notyfikacji korzystania z usługi chmurowej.***
    - *W ramach **Pośredniego stosowania Komunikatu** (np. gdy Zarządzający w usłudze chmury obliczeniowej przetwarza Informacje prawnie chronione powierzone przez Bank), notyfikacji dokonuje Powierzający podmiot nadzorowany (w w/w przypadku – Bank). Zarządzający uwzględnia ewentualne oczekiwania Powierzającego podmiotu nadzorowanego co do wsparcia w uzupełnieniu formularza stanowiącego załącznik nr 1 do Komunikatu.*

10. MIGRACJA DANYCH PRODUKCYJNYCH DO USŁUGI CHMURY OBLICZENIOWEJ

1. **Po poinformowaniu UKNF oraz upływie wymaganego przepisami prawa lub postanowieniami Komunikatu terminu, możliwe jest rozpoczęcie przetwarzania informacji w usłudze chmury obliczeniowej, w tym rozpoczęcie migracji danych produkcyjnych.** Po migracji danych powinny być przeprowadzone testy akceptacyjne.

Produkty

1. Dokumentacja migracji danych.

2. Wyniki testów potwierdzające jakość danych, **zabezpieczenia szyfrujące zgodnie z Komunikatem, procedury Disaster Recovery lub inne zabezpieczenia zgodne z Komunikatem i regulacjami wewnętrznymi Zarządzającego posiadającego licencję.**

11. URUCHOMIENIE PRODUKCYJNE

1. **Po zakończeniu i przetestowaniu migracji danych możliwe jest formalne uruchomienie produkcyjne**, poprzedzone udokumentowaną decyzją i komunikacją do użytkowników końcowych lub innych interesariuszy, zgodnie z regulacjami wewnętrznymi Zarządzającego.

Produkty

1. Udokumentowana decyzja o uruchomieniu usługi zgodnie z regulacjami wewnętrznymi Zarządzającego.

2. Komunikacja wewnętrzna Zarządzającego.

Załącznik 2. Wzorcowa dokumentacja klasyfikacji i oceny informacji

Tabela 1. Procedura klasyfikacji i oceny informacji

Nazwa i opis procesu										
Właściciel procesu										
Lp.	Kategoria informacji	Przykłady informacji	Charakter informacji (Informacja prawnie chroniona?)	Uwarunkowania prawne i kontraktowe	Ocena atrybutów bezpieczeństwa			Wartość informacji	Klasa informacji (z Tabeli 3.)	Dopuszczalność przetwarzania w chmurze obliczeniowej
					Poufność	Dostępność	Integralność			
1.										
2.										
3.										

Tabela 2. Matryca stosowanych zabezpieczeń

Dla każdej klasy informacji należy określić stosowane zabezpieczenia dla zachowania odpowiedniego poziomu ochrony w związku z poszczególnymi atrybutami bezpieczeństwa (np. szyfrowanie, multi factor authentication, backupy).

Atrybuty bezpieczeństwa	Stosowane zabezpieczenia				
	Klasa A	Klasa B	Klasa C	Klasa D	Klasa E
Poufność					
Integralność					
Dostępność					

Tabela 3. Klasy informacji

Klasa informacji	Zakres informacji objętych klasą
A	Klasa obejmuje informacje dostępne publicznie lub mogące podlegać ujawnieniu bez żadnych ograniczeń, a ich utrata nie skutkuje negatywnymi skutkami dla Zarządzającego.
B	Klasa obejmuje informacje, które mogą być ujawniane personelowi Zarządzającego, a w zakresie realizacji umowy outsourcingu także dostawcom / podwykonawcom Zarządzającego.
C	Klasa obejmuje informacje, które mogą być ujawniane jedynie uprawnionym osobom lub podmiotom, z zachowaniem szczególnych warunków.
D	Klasa obejmuje informacje, które objęte są tajemnicą prawnie chronioną i mogą być ujawniane jedynie uprawnionym osobom lub podmiotom, z zachowaniem szczególnych warunków.
E	Klasa obejmuje informacje, które nie mogą być ujawniane osobom lub podmiotom innym niż te, które wytworzyły informacje, najwyższemu kierownictwu i podmiotom przez nie wskazanym.

Załącznik 3. Przykład szablonu szacowania ryzyka

L.p.	Zagrożenie	Czynniki ograniczające ryzyko	Ocena ryzyka inherentnego		Poziom ryzyka inherentnego (N/Ś/K)*	Decyzja**	Plan postępowania z ryzykiem			
			Prawdo-podobieństwo	Wpływ			Proponowane zabezpieczenia obniżające ryzyko	Poziom ryzyka rezydualnego (N/Ś/K)*	Osoba odpowiedzialna	Termin wdrożenia
1.	Rozproszenie geograficzne przetwarzanych informacji (VI.2.1.a)									
2.	Możliwość utraty zgodności postępowania Zarządzającego posiadającego licencję z przepisami prawa (w tym wydanych licencji i/lub zezwoleń) (VI.2.1.b)									
3.	Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)									
4.	Jurysdykcja kraju, w którym odbywa się fizyczne przetwarzanie									

L.p.	Zagrożenie	Czynniki ograniczające ryzyko	Ocena ryzyka inherentnego		Poziom ryzyka inherentnego (N/Ś/K)*	Decyzja**	Plan postępowania z ryzykiem			
			Prawdo-podobieństwo	Wpływ			Proponowane zabezpieczenia obniżające ryzyko	Poziom ryzyka rezydualnego (N/Ś/K)*	Osoba odpowiedzialna	Termin wdrożenia
	(lokalizacja CDP) w zakresie dostępu do informacji przez organy administracji krajowej lub międzynarodowej (VI.2.1.d)									
5.	Przywiązanie do jednego dostawcy usług chmury obliczeniowej (VI.2.1.e)									
6.	Awarie i podatności elementów technologicznych chmury obliczeniowej (VI.2.1.f)									
7.	Podatność interfejsów zarządzających usługami (VI.2.1.g)									
8.	Ograniczona możliwość wpływania na zakres, kształt i									

L.p.	Zagrożenie	Czynniki ograniczające ryzyko	Ocena ryzyka inherentnego		Poziom ryzyka inherentnego (N/Ś/K)*	Decyzja**	Plan postępowania z ryzykiem			
			Prawdo-podobieństwo	Wpływ			Proponowane zabezpieczenia obniżające ryzyko	Poziom ryzyka rezydualnego (N/Ś/K)*	Osoba odpowiedzialna	Termin wdrożenia
	zmiany usług (VI.2.1.h)									
9.	Ograniczona możliwość kontrolowania dostawcy usług chmury obliczeniowej (VI.2.1.i)									
10.	Podział odpowiedzialności (VI.2.1.j)									
11.	Możliwość korzystania z usług w sposób niezgodny z intencjami Zarządzającego posiadającego licencję (VI.2.2.a)									
12.	Możliwość jednostronnej zmiany warunków technicznych korzystania z usługi (VI.2.2.b)									
13.	Stosowanie domyślnych lub									

L.p.	Zagrożenie	Czynniki ograniczające ryzyko	Ocena ryzyka inherentnego		Poziom ryzyka inherentnego (N/Ś/K)*	Decyzja**	Plan postępowania z ryzykiem			
			Prawdo-podobieństwo	Wpływ			Proponowane zabezpieczenia obniżające ryzyko	Poziom ryzyka rezydualnego (N/Ś/K)*	Osoba odpowiedzialna	Termin wdrożenia
	publicznie dostępnych parametrów konfiguracyjnych usług (VI.2.2.c)									
14.	Stosowane mechanizmy uwierzytelniania (VI.2.2.d)									
15.	Zasoby ludzkie (VI.2.3.a)									
16.	Zgodność środowiska technologicznego (VI.2.3.b)									
17.	Szyfrowanie informacji - zarządzanie kluczami (VI.2.5.b)									
18.	Szyfrowanie informacji - wykorzystywane algorytmy (VI.2.5.c)									
19.	Szyfrowanie informacji - "at rest" (VI.2.5.e)									

L.p.	Zagrożenie	Czynniki ograniczające ryzyko	Ocena ryzyka inherentnego		Poziom ryzyka inherentnego (N/Ś/K)*	Decyzja**	Plan postępowania z ryzykiem			
			Prawdo-podobieństwo	Wpływ			Proponowane zabezpieczenia obniżające ryzyko	Poziom ryzyka rezydualnego (N/Ś/K)*	Osoba odpowiedzialna	Termin wdrożenia
20.	Szyfrowanie informacji - "in transit" (VI.2.5.e)									
21.	Szyfrowanie informacji - kopie kluczy (utrata, poza kontrolą podmiotu nadzorowanego) (VI.2.5.f)									
22.	Kontrola „łańcucha outsourcingowego” - prawne wymogi (VI.2.6.a)									
23.	Kontrola „łańcucha outsourcingowego” - wykluczenia (VI.2.6.b)									
24.	Prawo właściwe umowy z dostawcą usługi chmury obliczeniowej (VI.2.8.a)									
25.	Opinia prawna dotycząca prawa państwa trzeciego (VI.2.8.b)									
26.	Inne istotne zagrożenia (VI.9) -									

L.p.	Zagrożenie	Czynniki ograniczające ryzyko	Ocena ryzyka inherentnego		Poziom ryzyka inherentnego (N/Ś/K)*	Decyzja**	Plan postępowania z ryzykiem			
			Prawdo-podobieństwo	Wpływ			Proponowane zabezpieczenia obniżające ryzyko	Poziom ryzyka rezydualnego (N/Ś/K)*	Osoba odpowiedzialna	Termin wdrożenia
	Spełnienie wymogów w zakresie RODO									
27.	Inne istotne zagrożenia - monitoring bezpieczeństwa (VI.9)									
28.	Inne istotne zagrożenia - anonimizacja danych (VI.9)									
29.	Inne istotne zagrożenia - badanie podatności technicznych (VI.9)									
30.	Inne istotne zagrożenia - bezpieczeństwo fizyczne CPD (VI.9)									

***Poziom ryzyka** – N – Niski, Ś – Średni, K – Krytyczny*

***Decyzja** – oznacza strategię postępowania z ryzykiem, która może obejmować: akceptację (zachowanie), redukcję (modyfikowanie), przeniesienie (dzielenie) lub unikanie ryzyka.*

Załącznik 4. Założenia metodyki w zakresie przetwarzania informacji w chmurze obliczeniowej zgodnie z Komunikatem

1. ZAŁOŻENIA OGÓLNE I ORGANIZACYJNE

1. Metodyka ma zastosowanie w przypadku Bezpośredniego stosowania Komunikatu, gdy informacje przetwarzane są przy użyciu chmury obliczeniowej publicznej lub hybrydowej (w zakresie jej części opartej o chmurę obliczeniową publiczną). Ponadto metodyka może być odpowiednio stosowana w ramach Pośredniego stosowania Komunikatu, w szczególności w zakresie realizacji czynności oczekiwanych od Zarządzającego przez Powierzający podmiot nadzorowany.
2. Zarządzający posiadający licencję przypisuje role i odpowiedzialności w procesie, poprzez zapewnienie co najmniej:

    a. udział właściciela procesu co najmniej w zakresie zgromadzenia wymaganych informacji o procesie oraz organizacyjnym;
    b. udział przedstawicieli jednostek odpowiedzialnych za bezpieczeństwo i compliance, co najmniej w charakterze doradczym (opiniodawczym) na etapie szacowania ryzyka i etapie faktycznego wdrażania usługi chmurowej i migracji oraz w procesie korzystania z usługi;
    c. udział przedstawicieli IT, co najmniej w charakterze doradczym (opiniodawczym) na etapie szacowania ryzyka technologicznego i etapie faktycznego wdrażania usługi chmurowej i migracji oraz w procesie korzystania z usługi;
    d. udział inspektora ochrony danych lub innej osoby wyznaczonej do nadzoru nad obszarem ochrony danych osobowych, co najmniej w charakterze doradczym (opiniodawczym) na etapie klasyfikacji i oceny informacji oraz szacowania ryzyka w zakresie zgodności z prawem ochrony danych osobowych oraz w procesie korzystania z usługi.
3. Należy zapewnić, by decyzja o migracji chmurowej i postępowaniu z ryzykiem chmurowym była podejmowana przez najwyższe kierownictwo Zarządzającego posiadającego licencję lub osoby przez nie upoważnione.
4. Należy zapewnić, by w każdym wypadku Zarząd Zarządzającego posiadającego licencję posiadał wiedzę o rozpoczęciu korzystania z usług chmury obliczeniowej.
5. Wszystkie czynności w ramach realizacji niniejszej metodyki powinny być dokumentowane w postaci pisemnej lub elektronicznej, w sposób zapewniający identyfikację osoby dokonującej czynności oraz integralność sporządzonej informacji.

2. INWENTARYZACJA (OPIS PROCESU)

1. Zarządzający posiadający licencję sporządza opis planowanego procesu, w ramach którego wykorzystywana ma być chmura obliczeniowa, określając możliwie precyzyjnie co najmniej:

    a. przebieg poszczególnych etapów procesu biznesowego, w ramach którego zakłada się korzystanie z chmury obliczeniowej;
    b. rodzaje zidentyfikowanych informacji, które mają być przetwarzane w usłudze chmury obliczeniowej i ich kategorie;
    c. skalę zakładanego przetwarzania wraz ze wskazaniem kryteriów przyjętych w tym zakresie;

d. zakładaną architekturę rozwiązania lub co najmniej wskazanie usług, z których Zarządzający posiadający licencję zamierza korzystać oraz zakładaną konfigurację – o ile dostępne są informacje pozwalające przyjąć określone założenia.

3. KLASYFIKACJA INFORMACJI

Cel: zapewnienie, że przetwarzane informacje uzyskują ochronę na odpowiednim poziomie, z uwzględnieniem właściwych wymogów prawnych.

1. Klasyfikacja informacji dokonywana jest w sposób usystematyzowany, w odniesieniu do konkretnej usługi chmurowej i konkretnego procesu podlegającego migracji do chmury.
2. Zarządzający posiadający licencję powinien wdrożyć i stosować klasyfikację informacji w oparciu o przyjęte przez siebie kryteria. Takie kryteria powinny uwzględniać co najmniej podział na informacje prawnie chronione w rozumieniu Komunikatu, informacje, których ochrona wynika z uregulowań prawnych oraz pozostałe informacje. Niniejsza metodyka zakłada wyróżnienie klas informacji w sposób przedstawiony w Tabeli nr 3 w Załączniku nr 2 do Standardu – Wzorcowa dokumentacja klasyfikacji i oceny informacji.
3. Przed przystąpieniem do procesu oceny informacji informacje zinwentaryzowane zgodnie z pkt. 2 niniejszej metodyki należy przypisać do odpowiednich klas determinujących poziom ochrony poszczególnych informacji.
4. W praktyce klasyfikacja informacji może uwzględniać atrybuty bezpieczeństwa, które podlegają ocenie pod kątem poufności, integralności i dostępności (zasad dostępu do informacji), przy uwzględnieniu skutków finansowych oraz regulacyjnych dla organizacji. Rekomendowane jest ponadto wskazanie minimalnych warunków zabezpieczeń obowiązujących w odniesieniu do poszczególnych klas informacji (przykład: Załącznik nr 2 do Standardu – Wzorcowa dokumentacja klasyfikacji i oceny informacji, Tabela nr 2).

4. OCENA INFORMACJI

Cel: ustalenie czy dopuszczalne jest przetwarzanie przez Zarządzającego posiadającego licencję poszczególnych zinwentaryzowanych i sklasyfikowanych grup informacji w usłudze chmury obliczeniowej.

1. Ocena informacji dokonywana jest w sposób usystematyzowany, w odniesieniu do konkretnej usługi chmurowej i konkretnego procesu, podlegającego migracji do chmury.
2. Ocena powinna obejmować co najmniej:

   a. uwzględnienie charakteru analizowanej informacji jako objętej lub nieobjętej tajemnicą prawnie chronioną oraz jako podlegającej innym uregulowaniu prawnym;
   b. uwzględnienie klas informacji i atrybutów bezpieczeństwa oraz właściwych dla tych klas standardów ochrony, przyporządkowanych zgodnie z pkt. 3 niniejszej metodyki;
   c. oszacowanie wartości informacji; dokonując oceny można wziąć pod uwagę następujące czynniki jako bezpośrednie i pośrednie skutki utraty kontroli nad ich przetwarzaniem:

      i. potencjalne kary finansowe,
      ii. szacowane koszty związane z identyfikacją i usuwaniem naruszenia,

iii. szacowane koszty i utracone przychody (utrata klientów, utrata informacji o środkach materialnych i niematerialnych itp.),
iv. szacowane koszty reputacyjne oraz wydatki poniesione na obszar public relations.

d. oszacowanie ważności informacji; dokonując oceny można wziąć pod uwagę abstrakcyjną (tj. nieodnoszącą się do konkretnego zagrożenia) ocenę wpływu na bezpieczeństwo informacji w oparciu o przyjęte przez Zarządzającego posiadającego licencję kryteria; ocena może odnosić się do skutków potencjalnego zagrożenia dla:

v. reputacji,
vi. finansów,
vii. ciągłości i niezawodności działania Zarządzającego posiadającego licencję oraz
viii. uprawnienia do prowadzenia działalności regulowanej przez Zarządzającego posiadającego licencję;

e. uwzględnienie skali prowadzonej działalności;
f. uwzględnienie odpowiedzialności za przetwarzane informacje;
g. uwzględnienie korporacyjnych, grupowych lub innych modeli oceny, które określają wspólne założenia dla grupy podmiotów, do których zalicza się Zarządzający posiadający licencję, jeśli mają one zastosowanie;
h. analizę występowania ograniczeń regulacyjnych mogących uniemożliwiać lub ograniczać korzystanie z chmury obliczeniowej (np. ograniczenia łańcucha outsourcingowego);
i. analizę występowania ograniczeń kontraktowych, mogących uniemożliwiać lub ograniczać korzystanie z chmury obliczeniowej (np. z uwagi na ograniczenia terytorialne, ograniczenia w zakresie korzystania z podwykonawców);
j. analizę występowania ograniczeń wewnątrzorganizacyjnych (np. wewnętrzne procedury ograniczające możliwość korzystania z chmury obliczeniowej dla określonych rodzajów informacji).

3. Ocena, o której mowa w pkt. 4.2. powyżej, powinna prowadzić do rozstrzygnięcia o dopuszczalności (lub niedopuszczalności) przetwarzania poszczególnych kategorii informacji w usłudze chmury obliczeniowej oraz wskazania ewentualnych warunków takiego korzystania, w szczególności z uwzględnieniem oceny czy dany proces obejmuje outsourcing szczególny w rozumieniu Komunikatu.
4. Klasyfikacja i ocena informacji powinna odbywać się cyklicznie, nie rzadziej niż raz na rok oraz za każdym razem:

a. dla każdej planowanej do wykorzystania lub wykorzystywanej usługi chmury obliczeniowej;
b. dla każdego nowego rodzaju informacji, który Zarządzający posiadający licencję zamierza przetwarzać w procesie;
c. po wystąpieniu następujących zdarzeń: zmiana prawa, regulacji, regulaminów lub postanowień umów, które to zmiany mogą wpływać na zgodność postępowania Zarządzającego posiadającego licencję w kontekście przetwarzania informacji w chmurze obliczeniowej;
d. zwiększenia lub zmniejszania skali przetwarzania informacji w procesie;
e. w przypadku istotnego zwiększenia wartości przetwarzanych informacji.

5. SZACOWANIE RYZYKA

Cel: identyfikacja ryzyk w obszarze prawnym, technologicznym i organizacyjnym wynikających z przetwarzania informacji w chmurze obliczeniowej, dobranie odpowiednich mitygantów oraz określenie planu zarządzania ryzykiem.

1. Zakres szacowania ryzyka (poziom szczegółowości analizy) powinien być określony zgodnie z zasadą proporcjonalności. W każdym jednak wypadku należy uwzględnić kroki opisane w niniejszym rozdziale.
2. Szacowanie ryzyka wymaga identyfikacji zagrożeń związanych z przetwarzaniem informacji w chmurze obliczeniowej, w szczególności zagrożeń, o których mowa w rozdziale VI. Komunikatu. Zagrożenia standardowo dotyczą w szczególności następujących obszarów ryzyka:

    a. lokalizacje przetwarzania (rozproszenie geograficzne);
    b. długość łańcucha outsourcingowego, zarządzanie poddostawcami.
    c. korzystanie z usług chmury obliczeniowej w sposób inny niż zamierzony;
    d. dostęp do informacji prawnie chronionej;
    e. kontrola nad danymi (własność danych);
    f. podatności interfejsów, błędy konfiguracji;
    g. zakres szyfrowania;
    h. kompetencje techniczne;
    i. vendor lock-in;
    j. poddanie umowy prawu obcemu lub obcej jurysdykcji;
    k. ograniczona kontrola nad przebiegiem współpracy z dostawcą, w tym ograniczenie uprawnień audytowych;
    l. adhezyjność warunków umowy z dostawcą.

3. Identyfikując zagrożenie należy wskazać jego źródło w ramach obszaru prawnego, organizacyjnego i technologicznego – w zakresie w jakim ma zastosowanie (np. postanowienia umowy, dokumentacja bezpieczeństwa, dostępna publicznie informacja o stwierdzonych podatnościach usługi).
4. Każde zagrożenie powinno zostać ocenione pod kątem wpływu jego wystąpienia na zgodność z wymaganiami prawnymi oraz wpływu na aspekty wskazane w pkt. 4.2. lit. d) powyżej., z uwzględnieniem kryteriów przyjętych przez Zarządzającego posiadającego licencję.
5. Każde zagrożenie powinno zostać ocenione pod kątem poziomu prawdopodobieństwa jego wystąpienia. Oceniając poziom prawdopodobieństwa, Zarządzający posiadający licencję powinien wziąć pod uwagę co najmniej wiedzę historyczną nt. wystąpienia podobnych zagrożeń, dostępną ekspercką wiedzę w tym zakresie oraz ustaloną zgodnie z pkt. 4.2. lit. c) wartość informacji.
6. Poziomowi wpływu oraz poziomowi prawdopodobieństwa można przypisać wartość liczbową, w celu ustalenia poziomu ryzyka początkowego, uzyskiwanego jako iloczyn tych dwóch wartości.
7. Zarządzający posiadający licencję może zidentyfikować interakcje między zagrożeniami (ich wzajemne wzmocnienia) lub przypisać określonym obszarom dodatkową wagę. W takim wypadku poziom ryzyka początkowego podlega odpowiedniemu podwyższeniu.
8. Dla każdego ryzyka początkowego na poziomie innym niż niski, określa się środki zaradcze wraz z osobami odpowiedzialnymi za ich stosowanie, a następnie – poziom ryzyka szczątkowego. Dla

każdego ryzyka szczątkowego określa się strategię zarządzania ryzykiem (np. w modelu: unikanie, redukcja, przenoszenie, akceptacja).

9. Wyniki szacowania ryzyka powinny być przeglądane regularnie, nie rzadziej niż raz do roku, oraz w każdym przypadku zajścia istotnych okoliczności mogących wpływać na poziom ryzyka.

6. ZGROMADZENIE DOKUMENTACJI I WERYFIKACJA ZGODNOŚCI

Cel: zagregowanie wszystkich wymogów, rozliczalność procesu.

1. W celu zapewnienia dostępności dokumentacji (m. in. na wypadek kontroli organu nadzoru) należy zgromadzić dokumentację wymaganą Komunikatem oraz przepisami prawa, w tym:

   m. plan przetwarzania informacji w chmurze obliczeniowej, plan ciągłości działania, przetestowany plan wyjścia;
   n. wypełniony szablon klasyfikacji i oceny informacji wraz z dokumentacją stanowiącą podstawę jego uzupełnienia (np. procedury wewnętrzne w zakresie stosowanych zabezpieczeń informacji) oraz
   o. wypełniony szablon szacowania ryzyka wraz z dokumentacją stanowiącą podstawę szacowania ryzyka (np. umowa z dostawcą i odpowiednia dokumentacja dostawcy, zamówione opinie prawne, wewnętrzna dokumentacja potwierdzająca posiadane kompetencje techniczne, dokumentacja środków bezpieczeństwa itd.) oraz plan postępowania z ryzykiem.

2. W zależności od wyników szacowania ryzyka oraz z uwzględnieniem zasady proporcjonalności Zarządzający posiadający licencję powinien zweryfikować, czy dodatkowo niezbędne jest udokumentowanie kwestii, o których mowa w rozdziale VII.9 Komunikatu, w szczególności o charakterze technologicznym.
3. Należy zweryfikować kompletność procesu w oparciu o checklistę wymogów określonych w Komunikacie oraz przepisach prawa.

7. DECYZJA O ROZPOCZĘCIU KORZYSTANIA Z USŁUGI CHMURY OBLICZENIOWEJ

1. Decyzję powinno podjąć najwyższe kierownictwo Zarządzającego posiadającego licencję lub osoba przez nie upoważniona.

8. INFORMOWANIE UKNF O KORZYSTANIU Z USŁUGI CHMURY OBLICZENIOWEJ

1. Notyfikacja UKNF o korzystaniu z usług chmury obliczeniowej powinna nastąpić w formie i zakresie odpowiadającym Załącznikowi nr 1 do Komunikatu – Informacja podmiotu nadzorowanego w sprawie przetwarzania informacji w chmurze obliczeniowej.
2. Przykładowe wypełnienie informacji do UKNF o rozpoczęciu korzystania z chmury obliczeniowej przez Zarządzającego posiadającego licencję stanowi Załącznik nr 7 do Standardu – Przykładowe wypełnienie informacji do UKNF o rozpoczęciu korzystania z chmury obliczeniowej przez Zarządzającego posiadającego licencję.

Załącznik 5. Wzorcowy plan przetwarzania informacji w chmurze obliczeniowej

1. INFORMACJE O REALIZOWANYCH ZADANIACH I PRZETWARZANYCH INFORMACJACH	
Nazwa systemu/aplikacji, w ramach którego/której przetwarzane są informacje	
Kategoria przetwarzanych informacji	☐ Chronione ☐ Niechronione
Klasa przetwarzanych informacji	☐ Publiczne ☐ Wewnętrzne ☐ Poufne ☐ Inne: ……
Typ przetwarzanych informacji	☐ Produkcyjne ☐ Testowe
Outsourcing szczególny chmury obliczeniowej	☐ Tak ☐ Nie
Opis formatu i struktury przetwarzanych informacji	
2. OCHRONA INFORMACJI	
Stosowane zabezpieczenia przetwarzanych informacji	☐ Maskowanie ☐ Pseudonimizacja ☐ Anonimizacja ☐ Inne: ……
Opis stosowanych zabezpieczeń przetwarzanych informacji	
Opis mechanizmów szyfrowania przetwarzanych informacji	
Zarządzanie i przechowywanie kluczy szyfrujących	☐ Zarządzający posiadający licencję ☐ Dostawca usługi chmury obliczeniowej
Opis kontroli dostępu do przetwarzanych informacji	…

3. UMOWA Z DOSTAWCĄ	
Dostawca	
Numer umowy	
Data zawarcia umowy	
Prawo właściwe dla umowy	
Okres obowiązywania umowy	
Data ostatniej zmiany w umowie	
Data rozpoczęcia korzystania z usługi	
4. INNE	
Data kolejnej weryfikacji planu	
Data ostatniej aktualizacji planu	
Zakres ostatniej aktualizacji planu	

**Szablon ma charakter przykładowy. Jego wypełnienie, zwłaszcza w pkt. 2 „Ochrona informacji", może następować poprzez odesłanie do innej dokumentacji funkcjonującej u Zarządzającego, przy czym odesłanie to powinno zostać sformułowane możliwie najbardziej precyzyjnie.*

Załącznik 6. Wzorcowy szablon scenariusza wyjścia z chmury

1. Opis usługi	
Identyfikator umowy	
Usługa (przedmiot umowy)	
Dostawca (nazwa/firma przedsiębiorcy)	
Planowana data zakończenia przetwarzania danych w chmurze obliczeniowej	
Okres wypowiedzenia umowy: a) przez Zarządzającego b) przez dostawcę	
2. Kryteria podjęcia decyzji o zastosowaniu scenariusza wyjścia z chmury obliczeniowej	
Kryteria długo i średnioterminowe	☐ obniżenie jakości usług lub pogorszenie kondycji finansowej dostawcy ☐ nieakceptowalna zmiana warunków świadczenia usługi przez dostawcę ☐ wypowiedzenie umowy przez dostawcę ☐ wewnętrzna decyzja biznesowa o zaprzestaniu korzystania z usługi lub zmiana strategii korzystania z usług zewnętrznych dostawców ☐ decyzja administracyjnej nakazująca Zarządzającemu posiadającemu licencję rozwiązanie umowy z dostawcą ☐ Inne: ……
Kryteria krótkoterminowe	☐ wystąpienie sytuacji awaryjnej wynikającej z utrzymującej się niedostępności usług przez okres dłuższy niż przewidziany w odpowiednich regulacjach wewnętrznych oraz braki perspektyw na przywrócenie normalnego funkcjonowania tych usług

	□ nagłe zaprzestanie prowadzenia działalności przez dostawcę □ wystąpienie poważnego incydentu skutkującego naruszeniem bezpieczeństwa usług i powierzonych danych
3. Sposób postępowania w związku z wygaśnięciem umowy	
Założona strategia	Przedłużenie relacji z dotychczasowym dostawcą: □ Zawarcie/przedłużenie umowy z dotychczasowym dostawcą Realizacja usługi przez inny podmiot: □ Wybór nowego dostawcy Realizacja usługi przez pozostałych, dotychczasowych dostawców: □ Kontynuacja z dotychczasowymi dostawcami Powrót działalności do Zarządzającego: □ Przejęcie działalności przez jednostkę Zarządzającego Zaprzestanie działalności: □ Brak kontynuowania działalności po wygaśnięciu umowy Inne: □..... □ .....
4. Kluczowe działania umożliwiające realizację scenariusza wyjścia	
Przedłużenie relacji	
Realizacja usługi przez inny podmiot	□ przeniesienie danych do alternatywnego dostawcy
Realizacja usługi przez Zarządzającego (powrót do Zarządzającego)	□ powrót danych do środowiska „on-premises”
Zaprzestanie działalności będącej przedmiotem umowy	□ zwrot danych przez dostawcę □ przeniesienie danych do alternatywnego dostawcy □ powrót danych do środowiska „on-premises”
Inne	
5. Zaangażowanie jednostki Zarządzającego realizujące scenariusze wyjścia	
Jednostki realizujące scenariusz	
Jednostki wspierające	
Jednostki informowane o wdrożeniu scenariusza	

6. Historia dokumentu		
Data utworzenia przeglądu/zmiany	Zatwierdzający	Komentarz / zakres zmian

Załącznik 7. Przykładowe wypełnienie informacji do UKNF o rozpoczęciu korzystania z chmury obliczeniowej przez Zarządzającego posiadającego licencję

Informacja podmiotu nadzorowanego w sprawie przetwarzania informacji w chmurze obliczeniowej

Oznaczenie podmiotu nadzorowanego (nazwa, adres, NIP, REGON)	Zarządzający wierzytelnościami S.A., ul. Zaległych wierzytelności 99, 00 – 001 Warszawa, NIP: 1234567890, REGON: 987654321

Zgodnie z postanowieniami *Komunikatu UKNF dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej*, informujemy o zamiarze przetwarzania / przetwarzaniu:

Rodzaj i zakres przetwarzanych informacji:	1. Informacje o pracownikach / współpracownikach Zarządzającego i TFI (skala przetwarzania – średnia): dane osobowe członków personelu, wizerunek, treść korespondencji e-mail; 2. informacje wynikające z umów przelewu wierzytelności (skala przetwarzania – duża): dane osób zadłużonych (w tym dane osobowe, w szczególności: imię, nazwisko, PESEL, płeć), treść korespondencji w zakresie obsługi osób zadłużonych, projekty ofert i umów, wyroki; 3. informacje o działalności Zarządzającego lub TFI (skala przetwarzania – duża): dane związane z procesem wyceny i zarządzania wierzytelnościami (w tym dane osobowe, w szczególności: imiona, nazwiska, numery dokumentów tożsamości, numery PESEL, numery telefonów, adresy e-mail dłużników).
Nazwa i adres dostawcy usług chmury obliczeniowej:	Chmura S.A., ul. Usługowa 90, 00 – 001 Warszawa

Nazwy usług chmury obliczeniowej lub ich rodzaj:	Serwery wirtualne, storage, sieci wirtualne, aplikacja CRM
Lokalizacje CPD przetwarzanych informacji (państwo, region):	Warszawa (Polska), Frankfurt (Niemcy), Dublin (Irlandia)
Data podpisania umowy z dostawcą usług chmury obliczeniowej lub przewidywany termin jej zawarcia:	10.2022 – przewidywany termin zawarcia umowy
Okres na jaki została zawarta umowa z dostawcą usług chmury obliczeniowej:	Na okres 3 lat od daty zawarcia umowy
Osoby do kontaktu w sprawie stosowania chmury obliczeniowej w podmiocie nadzorowanym (imię, nazwisko lub stanowisko, nr telefonu, adres e-mail):	Jan Kowalski, Dyrektor Departamentu IT, tel. 111 222 333, e-mail: jan.kowalski@zarządzający.pl

Oświadczamy, że postanowienia *Komunikatu UKNF dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej* zostały spełnione i skutecznie wdrożone.

Warszawa, 1 marca 2022 r. Członek Zarządu TFI Prokurent TFI

_____ _____

Miejscowość, data Podpisy osób reprezentujących podmiot nadzorowany

Załącznik 8. Analiza ISO 27001.

ISO27001 - opis kontroli po stronie dostawcy usługi chmury obliczeniowej

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.5.1.1	Polityki bezpieczeństwa informacji	Zabezpieczenie Zbiór polityk bezpieczeństwa informacji powinien być opracowany, zatwierdzony przez kierownictwo, opublikowany i zakomunikowany pracownikom i właściwym stronom zewnętrznym.	Tak	*Przykładowy opis*	Przykładowy opis	Samoocena	
A.5.1.2	Przegląd polityk bezpieczeństwa informacji	Zabezpieczenie Polityki bezpieczeństwa informacji należy poddawać przeglądom w zaplanowanych odstępach czasu lub wtedy, gdy wystąpią istotne zmiany, aby zapewnić, że nadal są właściwe, adekwatne i skuteczne.	Tak			Samoocena	
A.6.1.1	Role i odpowiedzialność za bezpieczeństwo informacji	Zabezpieczenie Odpowiedzialność za bezpieczeństwo informacji powinna być określona i przypisana.	Tak			Samoocena	
A.6.1.2	Rozdzielanie obowiązków	Zabezpieczenie Obowiązki i odpowiedzialności pozostające w konflikcie ze sobą należy rozdzielić, celem ograniczenia okazji do nieuprawnionej lub	Tak			Samoocena	

		nieumyślnej modyfikacji lub nadużycia organów organizacji.					
A.6.1.3	Kontakty z organami władzy	Zabezpieczenie Należy utrzymywać stosowne kontakty z właściwymi organami władzy.	Tak			Samoocena	
A.6.1.4	Kontakty z grupami zainteresowanych specjalistów	Zabezpieczenie Należy utrzymywać stosowne kontakty z grupami zainteresowanych specjalistów lub innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa.	Tak			Samoocena	
A.6.1.5	Bezpieczeństwo informacji w zarządzaniu projektami	Zabezpieczenie Bezpieczeństwo informacji należy uwzględnić w zarządzaniu projektami, niezależnie od rodzaju projektu.	Tak			Samoocena	
A.6.2.1	Polityka stosowania urządzeń mobilnych	Zabezpieczenie Należy wprowadzić politykę oraz wspierające ją zabezpieczenia w celu zarządzania ryzykami, wynikającymi z użytkowania urządzeń mobilnych.	Tak			Samoocena	
A.6.2.2	Telepraca	Zabezpieczenie Należy wdrożyć politykę oraz wspierające ją zabezpieczenia w celu ochrony informacji pobieranych, przetwarzanych i przechowywanych w miejscach wykonywania telepracy.	Tak			Samoocena	

A.7.1.1	Postępowanie sprawdzające	Zabezpieczenie Historię wszystkich kandydatów do pracy należy zweryfikować zgodnie z odpowiednimi przepisami prawnymi, regulacjami i zasadami etycznymi oraz proporcjonalnie do wymagań biznesowych, klasyfikacji informacji, do których będzie potrzebny dostęp oraz dostrzeżonych ryzyk	Tak			Samoocena	
A.7.1.2	Warunki zatrudnienia	Zabezpieczenie Umowy z pracownikami i kontrahentami powinny określać odpowiedzialność stron w obszarze bezpieczeństwa informacji	Tak			Samoocena	
A.7.2.1	Odpowiedzialność kierownictwa	Zabezpieczenie Kierownictwo powinno wymagać, aby wszyscy pracownicy i kontrahenci stosowali zasady bezpieczeństwa informacji zgodnie z obowiązującymi w organizacji politykami i procedurami	Tak			Samoocena	
A.7.2.2	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	Zabezpieczenie Wszyscy pracownicy organizacji oraz, w stosownych wypadkach, kontrahenci powinni przejść stosowne kształcenie i szkolenie uświadamiające oraz regularnie otrzymywać aktualizacje polityk i procedur związanych z ich stanowiskiem pracy	Tak			Samoocena	
A.7.2.3	Postępowanie dyscyplinarne	Zabezpieczenie Postępowanie dyscyplinarne wobec pracowników naruszających zasady bezpieczeństwa informacji należy prowadzić na podstawie ustalonych i przedstawionych im zasad	Tak			Samoocena	

A.7.3.1	Zakończenie zatrudnienia lub zmiana zakresu obowiązków	Zabezpieczenie Należy określić i przedstawić pracownikowi lub kontrahentowi, które odpowiedzialności i obowiązki w zakresie bezpieczeństwa informacji pozostaną aktualne po zakończeniu lub zmianie zatrudnienia, a następnie egzekwować je	Tak			Samoocena	
A.8.1.1	Inwentaryzacja aktywów	Zabezpieczenie Należy identyfikować aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów	Tak			Samoocena	
A.8.1.2	Własność aktywów	Zabezpieczenie Aktywa znajdujące się w ewidencji należy przypisać ich właścicielom	Tak			Samoocena	
A.8.1.3	Akceptowalne użycie aktywów	Zabezpieczenie Należy zidentyfikować, udokumentować i wdrożyć zasady akceptowalnego użycia informacji oraz aktywów związanych z informacjami i środkami przetwarzania informacji	Tak			Samoocena	
A.8.1.4	Zwrot aktywów	Zabezpieczenie Wszyscy pracownicy i użytkownicy podmiotów zewnętrznych, w momencie zakończenia zatrudnienia, umowy lub porozumienia, powinni zwrócić wszystkie posiadane aktywa organizacji	Tak			Samoocena	
A.8.2.1	Klasyfikowanie informacji	Zabezpieczenie: Informacje powinny być sklasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację	Tak			Samoocena	

A.8.2.2	Oznaczanie informacji	Zabezpieczenie Należy opracować i wdrożyć odpowiedni zbiór procedur oznaczania informacji, zgodnych z przyjętym w organizacji schematem klasyfikacji informacji	Tak			Samoocena	
A.8.2.3	Postępowanie z aktywami	Zabezpieczenie Należy opracować i wdrożyć procedury postępowania z aktywami, zgodnie z przyjętym przez organizację schematem klasyfikacji informacji	Tak			Samoocena	
A.8.3.1	Zarządzanie nośnikami wymiennymi	Zabezpieczenie Organizacja powinna wdrożyć procedury zarządzania nośnikami wymiennymi, zgodnie ze schematem klasyfikacji przyjętym w organizacji	Tak			Samoocena	
A.8.3.2	Wycofywanie nośników	Zabezpieczenie Nośniki, które nie będą dłużej wykorzystywane, należy bezpiecznie wycofać, zgodnie z formalnymi procedurami	Tak			Samoocena	
A.8.3.3	Przekazywanie nośników	Zabezpieczenie Nośniki zawierające informacje należy chronić przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu	Tak			Samoocena	
A.9.1.1	Polityka kontroli dostępu	Zabezpieczenie Politykę kontroli dostępu należy ustanowić, udokumentować i poddawać przeglądom zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji	Tak			Samoocena	
A.9.1.2	Dostęp do sieci i usług sieciowych	Zabezpieczenie Użytkownicy powinni mieć dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienia	Tak			Samoocena	

A.9.2.1	Rejestrowanie i wyrejestrowanie użytkowników	Zabezpieczenie W celu umożliwienia przydzielania praw dostępu należy wdrożyć formalny proces rejestrowania i wyrejestrowywania użytkowników	Tak			Samoocena	
A.9.2.2	Przydzielanie dostępu użytkownikom	Zabezpieczenie Należy wdrożyć formalny proces przydzielania dostępu użytkownikom w celu nadawania lub odbierania praw dostępu do wszystkich systemów i usług wszystkim kategoriom użytkowników	Tak			Samoocena	
A.9.2.3	Zarządzanie prawami uprzywilejowanego dostępu	Zabezpieczenie Przydzielanie i wykorzystanie praw uprzywilejowanego dostępu należy ograniczyć i nadzorować	Tak			Samoocena	
A.9.2.4	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	Zabezpieczenie Przydzielanie poufnych informacji uwierzytelniających powinno podlegać formalnemu procesowi zarządzania	Tak			Samoocena	
A.9.2.5	Przegląd praw dostępu użytkowników	Zabezpieczenie Właściciele aktywów powinni przeglądać prawa dostępu użytkowników w regularnych odstępach czasu	Tak			Samoocena	
A.9.2.6	Odbieranie lub dostosowywanie praw dostępu	Zabezpieczenie Przydzielone pracownikom i użytkownikom zewnętrznym prawa dostępu do informacji i środków przetwarzania informacji należy odbierać po zakończeniu zatrudnienia, umowy lub porozumienia, lub dostosowywać do zaistniałych zmian	Tak			Samoocena	

A.9.3.1	Stosowanie poufnych informacji uwierzytelniających	Zabezpieczenie Użytkownicy powinni mieć obowiązek przestrzegania przyjętych w organizacji zasad stosowania poufnych informacji uwierzytelniających	Tak			Samoocena	
A.9.4.1	Ograniczenie dostępu do informacji	Zabezpieczenie Dostęp do informacji oraz funkcji systemu aplikacyjnego należy ograniczać zgodnie z polityką kontroli dostępu	Tak			Samoocena	
A.9.4.2	Procedury bezpiecznego logowania	Zabezpieczenie Tam, gdzie polityka kontroli dostępu tego wymaga, dostęp do systemów i aplikacji powinien być kontrolowany przez procedurę bezpiecznego logowania	Tak			Samoocena	
A.9.4.3	System zarządzania hasłami	Zabezpieczenie Systemy zarządzania hasłami powinny być interaktywne i zapewniać wybór haseł dobrej jakości	Tak			Samoocena	
A.9.4.4	Użycie uprzywilejowanych programów narzędziowych	Zabezpieczenie Wykorzystanie programów narzędziowych, umożliwiających obejście zabezpieczeń systemów i aplikacji, powinno podlegać ograniczeniom i ścisłemu nadzorowi	Tak			Samoocena	
A.9.4.5	Kontrola dostępu do kodów źródłowych programów	Zabezpieczenie Dostęp do kodu źródłowego programów powinien być ograniczony	Tak			Samoocena	
A.10.1.1	Polityka stosowania zabezpieczeń kryptograficznych	Zabezpieczenie Należy opracować i wdrożyć politykę stosowania zabezpieczeń kryptograficznych do ochrony informacji	Tak			Samoocena	

A.10.1.2	Zarządzanie kluczami	Zabezpieczenie Należy opracować politykę dotyczącą korzystania, ochrony i okresów ważności kluczy kryptograficznych i wdrożyć ją na wszystkich etapach cyklu życia kluczy	Tak			Samoocena	
A.11.1.1	Fizyczna granica obszaru bezpiecznego	Zabezpieczenie Należy określić granice bezpieczeństwa i wykorzystać je do zabezpieczenia obszarów zawierających wrażliwe lub krytyczne informacje oraz środki przetwarzania informacji	Tak			Samoocena	
A.11.1.2	Fizyczne zabezpieczenie wejść	Zabezpieczenie Bezpieczne strefy należy chronić odpowiednimi zabezpieczeniami wejść zapewniającymi dostęp wyłącznie osobom uprawnionym	Tak			Samoocena	
A.11.1.3	Zabezpieczenie biur, pomieszczeń i obiektów	Zabezpieczenie Należy zaprojektować i stosować fizyczne zabezpieczenia biur, pomieszczeń i obiektów	Tak			Samoocena	
A.11.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	Zabezpieczenie należy zaprojektować i stosować fizyczne zabezpieczenia przed katastrofami naturalnymi, wrogim atakiem lub wypadkami	Tak			Samoocena	
A.11.1.5	Praca w obszarach bezpiecznych	Zabezpieczenie Należy zaprojektować i stosować procedury pracy w obszarach bezpiecznych	Tak			Samoocena	
A.11.1.6	Obszary dostaw i załadunku	Zabezpieczenie Należy sprawować nadzór nad punktami dostępu takimi jak obszary dostaw i załadunku oraz innymi punktami, przez które nieuprawnione osoby mogą wejść do pomieszczeń i, jeśli to możliwe, odizolować je od środków przetwarzania informacji, aby zapobiec nieuprawnionemu dostępowi	Tak			Samoocena	

A.11.2.1	Lokalizacja i ochrona sprzętu	Zabezpieczenie Sprzęt należy umieścić i chronić w taki sposób, aby zredukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazje do nieuprawnionego dostępu	Tak			Samoocena	
A.11.2.2	Systemy wspomagające	Zabezpieczenia Sprzęt należy chronić przed awariami zasilania oraz innymi przerwami spowodowanymi awariami systemów wspomagających	Tak			Samoocena	
A.11.2.3	Bezpieczeństwo okablowania	Zabezpieczenie Okablowanie zasilające oraz telekomunikacyjne, przenoszące dane lub wspomagające usługi informacyjne należy chronić przez przechwyceniem, zakłóceniem lub uszkodzeniem	Tak			Samoocena	
A.11.2.4	Konserwacja sprzętu	Zabezpieczenie Sprzęt należy prawidłowo konserwować w celu zapewnienia jego ciągłej dostępności i integralności	Tak			Samoocena	
A.11.2.5	Wynoszenie aktywów	Zabezpieczenie Sprzętu, informacji i programów nie należy wynosić poza siedzibę organizacji bez uzyskania wcześniejszego zezwolenia	Tak			Samoocena	
A.11.2.6	Bezpieczeństwo sprzętu i aktywów poza siedzibą	Zabezpieczenie Aktywa wynoszone poza siedzibę organizacji należy zabezpieczyć przed wystąpieniem różnych ryzyk związanych z pracą poza siedzibą	Tak			Samoocena	
A.11.2.7	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	Zabezpieczenie Przed zbyciem lub przekazaniem sprzętu do ponownego użycia należy sprawdzić wszystkie jego składniki zawierające nośniki informacji, dla zapewnienia, że wszystkie wrażliwe dane i	Tak			Samoocena	

		licencjonowane programy zostały usunięte lub bezpiecznie nadpisane					
A.11.2.8	Pozostawianie sprzętu użytkownika bez opieki	Zabezpieczenie Użytkownicy powinni zapewnić odpowiednią ochronę sprzętu pozostawianego bez opieki	Tak			Samoocena	
A.11.2.9	Polityka czystego biurka i ekranu	Zabezpieczenie Należy wprowadzić politykę czystego biurka dla dokumentów papierowych i przenośnych nośników pamięci oraz politykę czystego ekranu dla środków przetwarzania informacji	Tak			Samoocena	
A.12.1.1	Dokumentowanie procedur eksploatacyjnych	Zabezpieczenie Procedury eksploatacyjne powinny być udokumentowane i udostępniane wszystkim potrzebującym ich użytkownikom	Tak			Samoocena	
A.12.1.2	Zarządzanie zmianami	Zabezpieczenie Zmiany w organizacji, procesach biznesowych, środkach przetwarzania informacji i systemach, które mają wpływ na bezpieczeństwo informacji, powinny być nadzorowane	Tak			Samoocena	
A.12.1.3	Zarządzanie pojemnością	Zabezpieczenie Należy monitorować i dostosowywać wykorzystanie zasobów oraz przewidywać wymaganą pojemność w przyszłości, dla zapewnienia właściwej wydajności systemu	Tak			Samoocena	
A.12.1.4	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	Zabezpieczenie Należy oddzielić środowiska rozwojowe, testowe i produkcyjne celem redukcji ryzyk związanych z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym	Tak			Samoocena	

A.12.2.1	Zabezpieczenia przed szkodliwym oprogramowaniem	Zabezpieczenie Należy wdrożyć zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przed szkodliwym oprogramowaniem, w połączeniu z właściwym uświadamianiem użytkowników	Tak			Samoocena	
A.12.3.1	Zapasowe kopie informacji	Zabezpieczenie Zapasowe kopie informacji, oprogramowania i obrazów systemów należy regularnie wykonywać i testować, zgodnie z ustaloną polityką kopii zapasowych	Tak			Samoocena	
A.12.4.1	Rejestrowanie zdarzeń	Zabezpieczenie Należy tworzyć, przechowywać i systematycznie przeglądać dzienniki zdarzeń rejestrujące działania użytkowników, wyjątki, usterki oraz zdarzenia związane z bezpieczeństwem informacji	Tak			Samoocena	
A.12.4.2	Ochrona informacji w dziennikach zdarzeń	Środki służące rejestrowaniu zdarzeń oraz informacje w dziennikach zdarzeń należy chronić przed manipulacją i nieuprawnionym dostępem	Tak			Samoocena	
A.12.4.3	Rejestrowanie działań administratorów i operatorów	Zabezpieczenie Działania administratorów i operatorów systemów należy rejestrować, a dzienniki chronić i systematycznie przeglądać	Tak			Samoocena	
A.12.4.4	Synchronizacja zegarów	Zabezpieczenie Zegary wszystkich istotnych systemów przetwarzania informacji w organizacji lub domenie bezpieczeństwa należy zsynchronizować z jednym wzorcowym źródłem czasu	Tak			Samoocena	

A.12.5.1	Instalacja oprogramowania w systemach produkcyjnych	Zabezpieczenie Należy wdrożyć procedury nadzoru nad instalacją oprogramowania w systemach produkcyjnych	Tak			Samoocena	
A.12.6.1	Zarządzanie podatnościami technicznymi	Zabezpieczenie Informacje o podatnościach technicznych wykorzystywanych systemów informacyjnych należy niezwłocznie pozyskiwać, oceniać stopień narażenia organizacji na te podatności i podejmować odpowiednie środki w celu przeciwdziałania związanemu z nimi ryzyku	Tak			Samoocena	
A.12.6.2	Ograniczenia w instalowaniu oprogramowania	Zabezpieczenie Należy ustanowić i wdrożyć zasady instalowania oprogramowania przez użytkowników	Tak			Samoocena	
A.12.7.1	Zabezpieczenia audytu systemów informacyjnych	Zabezpieczenie Należy starannie zaplanować i uzgodnić wymagania audytu oraz działania obejmujące weryfikację systemów produkcyjnych, w celu zminimalizowania zakłóceń w procesach biznesowych	Tak			Samoocena	
A.13.1.1	Zabezpieczenia sieci	Zabezpieczenie Sieci powinny być zarządzane i nadzorowane, w celu ochrony informacji w systemach i aplikacjach	Tak			Samoocena	
A.13.1.2	Bezpieczeństwo usług sieciowych	Zabezpieczenie Umowy dotyczące wszystkich usług sieciowych, świadczonych wewnętrznie lub zlecanych na zewnątrz, powinny zawierać zidentyfikowane mechanizmy zabezpieczeń, poziomy świadczenia usług i wymagania dotyczące zarządzania	Tak			Samoocena	

A.13.1.3	Rozdzielanie sieci	Zabezpieczenie Grupy usług informacyjnych, użytkowników i systemów informacyjnych powinny być rozdzielone w strukturze sieci	Tak			Samoocena	
A.13.2.1	Polityki i procedury przesyłania informacji	Zabezpieczenie Należy wdrożyć formalne polityki przesyłania informacji, procedury i zabezpieczenia w celu ochrony informacji przesyłanych przy użyciu wszystkich rodzajów środków łączności.	Tak			Samoocena	
A.13.2.2	Porozumienia dotyczące przesyłania informacji	Zabezpieczenie Porozumienia powinny uwzględniać bezpieczne przesyłanie informacji biznesowych między organizacją i podmiotami zewnętrznymi.	Tak			Samoocena	
1.13.2.3	Wiadomości elektroniczne	Zabezpieczenie Informacje przekazywane w formie wiadomości elektronicznych powinny być odpowiednio chronione.	Tak			Samoocena	
A.13.2.4	Umowy o zachowaniu poufności	Zabezpieczenie Należy zidentyfikować, regularnie przeglądać i dokumentować wymagania odnoszące się do umów o zachowaniu poufności lub nieujawnianiu informacji, w sposób odzwierciedlający potrzeby organizacji w zakresie ochrony informacji.	Tak			Samoocena	
A.14.1.1	Analiza i specyfikacja wymagań bezpieczeństwa informacji	Zabezpieczenie Wymagania dotyczące bezpieczeństwa informacji należy włączyć do wymagań stawianych nowym systemom informacyjnym lub rozbudowie systemów istniejących.	Tak			Samoocena	

A.14.1.2	Zabezpieczenie usług aplikacyjnych w sieciach publicznych	Zabezpieczenie Informacje przesyłane w sieciach publicznych, związane z usługami świadczonymi przez aplikacje, należy chronić przed nieuczciwymi działaniami, sporami dotyczącymi umów oraz nieuprawnieniem i zmianami.	Tak			Samoocena	
A.14.1.3	Ochrona transakcji usług aplikacyjnych	Zabezpieczenie Informacje związanie z transakcjami dokonywanymi w ramach usług świadczonych przez aplikacje należy chronić, aby zapobiec przerwaniu transmisji, błędom w trasowaniu, nieuprawnionym zmianom wiadomości, nieuprawnionemu ujawnieniu, nieuprawnionemu powieleniu lub odtworzeniu.	Tak			Samoocena	
A.14.2.1	Polityka bezpieczeństwa prac rozwojowych	Zabezpieczenie Należy ustanowić zasady prac nad rozwojem oprogramowania i systemów oraz stosować je w pracach rozwojowych prowadzonych wewnątrz organizacji.	Tak			Samoocena	
A.14.2.2	Procedury kontroli zmian w systemach	Zabezpieczenie Należy nadzorować zmiany w systemach podczas ich cyklu rozwojowego, przy użyciu formalnych procedur kontroli zmian.	Tak			Samoocena	
A.14.2.3	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	Zabezpieczenie Po dokonaniu zmian w platformach produkcyjnych należy przeprowadzić przegląd krytycznych aplikacji biznesowych lub przetestować je, aby uzyskać pewność, że zmiany nie miały niekorzystnego wpływu na działalność organizacji lub bezpieczeństwo.	Tak			Samoocena	

A.14.2.4	Ograniczenia dotyczące zmian w systemach oprogramowania	Zabezpieczenie modyfikacji w pakietach oprogramowania należy dokonywać z rozwagą i ograniczać się do zmian niezbędnych, a wszystkie takie zmiany ściśle nadzorować.	Tak			Samoocena	
A.14.2.5	Zasady projektowania bezpiecznych systemów	Zabezpieczenie Należy ustanowić, udokumentować i utrzymywać zasady projektowania bezpiecznych systemów oraz stosować je do wszystkich prac implementacyjnych nad systemami informacyjnymi.	Tak			Samoocena	
A.14.2.6	Bezpieczne środowisko rozwojowe	Zabezpieczenie Organizacje powinny ustanowić i odpowiednio chronić bezpieczne środowiska rozwojowe przeznaczone do rozwoju systemów oraz prac integracyjnych obejmujących całość cyklu rozwojowego procesów.	Tak			Samoocena	
A.14.2.7	Prace rozwojowe zlecane podmiotom zewnętrznym	Zabezpieczenie Organizacja powinna nadzorować i monitorować prace rozwojowe nad systemami zlecone podmiotom zewnętrznym.	Tak			Samoocena	
A.14.2.8	Testowanie bezpieczeństwa systemów	Zabezpieczenie Funkcje bezpieczeństwa należy testować w czasie prac rozwojowych.	Tak			Samoocena	
A.14.2.9	Testy akceptacyjne systemów	Zabezpieczenie Dla nowych systemów informacyjnych, ich modernizacji i nowych wersji systemów należy ustanowić programy testów akceptacyjnych i kryteria z nimi związane.	Tak			Samoocena	
A.14.3.1	Ochrona danych testowych	Zabezpieczenie Dane testowe należy starannie wybierać, chronić i nadzorować.	Tak			Samoocena	

A.15.1.1	Polityka bezpieczeństwa informacji w relacjach z dostawcami	Zabezpieczenie Należy uzgodnić z dostawcą i udokumentować wymagania bezpieczeństwa informacji celem zmniejszenia ryzyk związanych z dostępem Dostawcy do aktywów organizacji.	Tak			Samoocena	
A.15.1.2	Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami	Zabezpieczenie Należy ustanowić wszystkie istotne wymagania dotyczące bezpieczeństwa informacji i uzgodnić je z każdym dostawcą, który może uzyskać dostęp, przetwarzać, przechowywać, przesyłać lub dostarczać elementy infrastruktury teleinformatycznej dla przetwarzania informacji należących do organizacji.	Tak			Samoocena	
A.15.1.3	Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych	Zabezpieczenie Porozumienia z dostawcami powinny uwzględniać wymagania odnoszące się do ryzyk w bezpieczeństwie informacji, związanych z usługami technologii informacyjnych i telekomunikacyjnych oraz łańcuchem dostaw produktów.	Tak			Samoocena	
A.15.2.1	Monitorowanie i przegląd usług świadczonych przez dostawców	Zabezpieczenie Organizacje powinny regularnie monitorować, przeglądać i audytować dostarczanie usług zewnętrznych.	Tak			Samoocena	
A.15.2.2	Zarządzanie zmianami w usługach świadczonych przez dostawców	Zabezpieczenie Należy zarządzać zmianami w zakresie świadczenia usług przez dostawców, w tym utrzymaniem i doskonaleniem istniejących polityk bezpieczeństwa informacji, procedur i zabezpieczeń, z uwzględnieniem krytyczności informacji, systemów i procesów biznesowych,	Tak			Samoocena	

		których dotyczą oraz ponownego szacowania ryzyka.					
A.16.1.1	Odpowiedzialność i procedury	Zabezpieczenie Należy ustanowić odpowiedzialność kierownictwa oraz procedury zapewniające szybką, skuteczną i zorganizowaną reakcję na incydenty związane z bezpieczeństwem informacji.	Tak			Samoocena	
A.16.1.2	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Zabezpieczenie Zdarzenie związane z bezpieczeństwem informacji należy zgłaszać odpowiednimi kanałami zarządczymi tak szybko, jak tylko to jest możliwe.	Tak			Samoocena	
A.16.1.3	Zgłaszanie słabości związanych z bezpieczeństwem informacji	Zabezpieczenie Należy zobowiązać pracowników oraz kontrahentów korzystających z systemów usług informacyjnych organizacji do odnotowania i zgłaszania wszelkich zaobserwowanych lub podejrzewanych słabości związanych z bezpieczeństwem informacji w systemach lub usługach.	Tak			Samoocena	
A.16.1.4	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	Zabezpieczenie Zdarzenia związane z bezpieczeństwem informacji należy ocenić i podjąć decyzję w sprawie zakwalifikowania ich jako incydentów związanych z bezpieczeństwem informacji.	Tak			Samoocena	
A.16.1.5	Reagowanie na incydenty związane z	Zabezpieczenie Reakcja na incydenty związane z	Tak			Samoocena	

	bezpieczeństwem informacji	bezpieczeństwem informacji powinna być zgodna z udokumentowanymi procedurami.					
A.16.1.6	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	Zabezpieczenie Wiedzę zdobyta podczas analizy i rozwiązywania incydentów związanych z bezpieczeństwem informacji należy wykorzystać do zredukowania prawdopodobieństwa wystąpienia lub skutków przyszłych incydentów.	Tak			Samoocena	
A.16.1.7	Gromadzenie materiału dowodowego	Zabezpieczenie Organizacja powinna określić i stosować procedury identyfikacji, gromadzenia, pozyskiwania i utrwalania informacji, które mogą stanowić materiał dowodowy.	Tak			Samoocena	
A.17.1.1	Planowanie ciągłości bezpieczeństwa informacji	Zabezpieczenie Organizacja powinna określić wymagania dotyczące bezpieczeństwa informacji i ciągłości zarządzania bezpieczeństwem informacji w niekorzystnych sytuacjach np. w czasie kryzysu czy katastrofy	Tak			Samoocena	
A.17.1.2	Wdrożenie ciągłości bezpieczeństwa informacji	Zabezpieczenie Organizacja powinna ustanowić, udokumentować, wdrożyć i utrzymywać procesy, procedury i zabezpieczenia dla zapewnienia w niekorzystnej sytuacji wymaganego poziomu ciągłości bezpieczeństwa informacji.	Tak			Samoocena	
A.17.1.3	Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji	Zabezpieczenie Organizacja powinna weryfikować ustanowione i wdrożone zabezpieczenia ciągłości bezpieczeństwa informacji w regularnych odstępach czasu celem zapewnienia ich	Tak			Samoocena	

		aktualności i skuteczności w niekorzystnych sytuacjach.					
A.17.2.1	Dostępność środków przetwarzania informacji	Zabezpieczenie Środki przetwarzania informacji należy wdrażać z nadmiarem wystarczającym do spełnienia wymagań dostępności.	Tak			Samoocena	
A.18.1.1	Określenie stosownych wymagań prawnych i umownych	Zabezpieczenie Wszystkie istotne wymagania prawne, regulacyjne, umowne oraz podejście organizacji do ich przestrzegania należy zidentyfikować, udokumentować i aktualizować dla każdego systemu informacyjnego oraz całości organizacji.	Tak			Samoocena	
A.18.1.2	Prawa własności intelektualnej	Należy wdrożyć odpowiednie procedury zapewniające zgodność z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania.	Tak			Samoocena	
A.18.1.3	Ochrona zapisów	Zabezpieczenie Zapisy należy chronić przed utratą, zniszczeniem, fałszowaniem, nieuprawnionym dostępem i nieuprawnionym opublikowaniem, stosownie do wymagań prawnych, regulacyjnych, umownych i biznesowych.	Tak			Samoocena	
A.18.1.4	Prywatność i ochrona danych identyfikujących osobę	Zabezpieczenie Należy zapewnić prywatność i ochronę danych identyfikujących osobę stosownie do odpowiednich przepisów prawa i regulacji.	Tak			Samoocena	

A.18.1.5	Regulacje dotyczące zabezpieczeń kryptograficznych	Zabezpieczenie Zabezpieczenia kryptograficzne należy stosować zgodnie z odpowiednimi umowami, przepisami i regulacjami	Tak			Samoocena	
A.18.2.1	Niezależny przegląd bezpieczeństwa informacji	Zabezpieczenie Podejście organizacji do zarządzania bezpieczeństwem informacji oraz jego wdrożenie (tzn. cele stosowania zabezpieczeń, zabezpieczenia, polityki, procesy i procedury dotyczące bezpieczeństwa informacji) należy poddawać niezależnemu przeglądowi w zaplanowanych odstępach czasu lub wtedy, gdy nastąpią istotne zmiany.	Tak			Samoocena	
A.18.2.2	Zgodność z politykami bezpieczeństwa i standardami	Zabezpieczenie Kierownicy powinni regularnie dokonywać przeglądu zgodności przetwarzania informacji i procedur z odpowiednimi politykami bezpieczeństwa, standardami i innymi wymaganiami dotyczącymi bezpieczeństwa, w zakresie przydzielonej im odpowiedzialności.	Tak			Samoocena	
A.18.2.3	Sprawdzania zgodności technicznej	Zabezpieczenie Należy regularnie przeglądać systemy informacyjne celem sprawdzenia ich zgodności z politykami bezpieczeństwa informacji i standardami obowiązującymi w organizacji.	Tak			Samoocena	

Załącznik 9. Wytyczne do opracowania planu ciągłości działania.

Niniejszy wytyczne opisują przykładowe elementy jakie należy wziąć pod uwagę przy opracowywaniu planu ciągłości działania w kontekście przetwarzania informacji w chmurze obliczeniowej w ramach Bezpośredniego stosowania Komunikatu. Zarządzający posiadający licencję powinien traktować poniższy dokument wyłącznie jako materiał pomocniczy i w razie potrzeby dostosować go do swoich potrzeb z uwzględnieniem specyfiki danej organizacji oraz danej usługi chmury obliczeniowej.

1. Udokumentowany plan ciągłości działania Zarządzającego posiadającego licencję powinien określać jego sposób funkcjonowania w przypadku zaistnienia zdarzeń, które mogą skutkować niedostępnością lub utratą zasobów Zarządzającego posiadającego licencję w związku z korzystaniem z chmury publicznej lub hybrydowej. W szczególności powinien on uwzględniać możliwość utraty kontroli przez Zarządzającego posiadającego licencję nad przetwarzanymi informacjami u danego dostawcy usług chmury obliczeniowej oraz możliwość przerwania ciągłości działania usługi chmury obliczeniowej zapewnianej przez tego dostawcę.
2. Wskazane jest, aby plan ciągłości działania określał sposób zabezpieczenia usług krytycznych Zarządzającego posiadającego licencję oraz danych przetwarzanych w chmurze (np. poprzez określenie dodatkowego miejsca składowania backupów i kopii zapasowych o krytycznych znaczeniu), a także zawierał opis rozwiązań alternatywnych i zastępczych, które można wykorzystać w sytuacjach kryzysowych.
3. W zakresie możliwości utraty kontroli nad przetwarzanymi informacjami u danego dostawcy usług chmury obliczeniowej Zarządzający posiadający licencję powinien uwzględnić w przyjętym planie ciągłości działania co najmniej:
    a. sposoby zabezpieczenia danych kluczowych z perspektywy ciągłości funkcjonowania oraz dalszej działalności operacyjnej. Zarządzający posiadający licencję powinien (przynajmniej w odniesieniu do danych, których niedostępność może bezpośrednio wpłynąć na powstawanie strat finansowych bądź wizerunkowych bądź uniemożliwić lub znacząco utrudnić kontynuację działalności przez Zarządzającego posiadającego licencję) zapewnić dywersyfikację przechowywania tych informacji w przynajmniej jednym niezależnym od dostawcy usług chmury obliczeniowej ośrodku. Możliwość łatwego i szybkiego skorzystania z danych zapasowych, a także ich kompletność do celów zapewnienia ciągłości działania powinny być poddawane regularnym testom;
    b. potencjalny i akceptowalny przez Zarządzającego posiadającego licencję poziom utraty danych wyrażony w jednostce czasu (Recovery Point Objective – RPO);
    c. strategię postępowania względem osób, których dotyczą dane osobowe oraz względem Prezesa Urzędu Ochrony Danych Osobowych – na wypadek, gdyby utrata kontroli nad przetwarzanymi informacjami wiązała się z naruszeniem lub możliwością naruszenia ochrony danych osobowych;
    d. strategię postępowania względem wszelkich innych roszczeń, jakie mogą być kierowane względem Zarządzającego posiadającego licencję w związku z utratą

kontroli nad przetwarzanymi informacjami u danego dostawcy usług chmury obliczeniowej.

4. W odniesieniu do możliwości przerwania ciągłości działania usługi chmury obliczeniowej wskazane jest, aby Zarządzający posiadający licencję uwzględnił w przyjętym planie ciągłości działania co najmniej następujące elementy:
    a. w razie uwzględnienia w planie ciągłości działania dwóch lub więcej chmur obliczeniowych lub dwóch lub więcej dostawców usług chmury obliczeniowej - weryfikację własnej zdolności do utrzymania deklarowanych założeń w ramach przejętego planu ciągłości działania. W szczególności Zarządzający posiadający licencję powinien dokonać weryfikacji zgodności konfiguracji usług i odtwarzalności środowiska teleinformatycznego;
    b. zasady komunikacji z podmiotami korzystającymi z usług Zarządzającego posiadającego licencję, w razie, gdy przerwanie ciągłości działania usługi chmury obliczeniowej doprowadzi do zaburzenia ciągłości świadczonych usług;
    c. strategię postępowania względem wszelkich roszczeń jakie mogą być kierowane względem Zarządzającego posiadającego licencję w związku z przerwaniem ciągłości działania usługi chmury obliczeniowej.
5. Przyjęty przez Zarządzającego posiadającego licencję plan ciągłości działania w odniesieniu do wszelkich potencjalnych ryzyk powinien określać minimalne cele ciągłości działania rozumiane jako minimalny poziom funkcjonowania usług, który jest akceptowalny przez Zarządzającego posiadającego licencję dla osiągnięcia celów jego działalności w trakcie wystąpienia zakłócenia (Minimum Business Continuity Objective - MBCO).
6. Dla osiągnięcia MBCO, Zarządzający posiadający licencję powinien określić czas, jaki jest niezbędny do przywrócenia usługi do MBCO od chwili zaobserwowania przerwania działania usług na skutek zaistniałego zdarzenia. Wskazane jest zarazem zapewnienie możliwości przełączenia usług Zarządzającego posiadającego licencję do zewnętrznego ośrodka względem dostawcy usług chmury obliczeniowej.
7. Zarządzający posiadający licencję powinien wydzielić zespół kryzysowy, powoływany w razie wystąpienia istotnego zakłócenia jego działalności. Skład i kompetencje zespołu kryzysowego powinny umożliwiać natychmiastowe podjęcie wszelkich działań mających na celu zapobiec awarii i zapewnić ciągłość działania Zarządzającego posiadającego licencję, w tym koordynację działań zapobiegawczych i nawiązywanie współpracy z podmiotami zewnętrznymi, z którymi współpraca okaże się niezbędna dla przywrócenia prawidłowego funkcjonowania Zarządzającego posiadającego licencję.
8. Plan ciągłości działania powinien być poddawany regularnym przeglądom pod kątem jego adekwatności i skuteczności w kontekście zapewnienia ciągłego i niezakłóconego prowadzenia działalności przez Zarządzającego posiadającego licencję i w razie potrzeby modyfikowany. Niezależnie od regularnych przeglądów, wskazane jest, aby Zarządzający posiadający licencję dokonał przeglądu planu po każdym incydencie wpływającym na swoją ciągłość działania oraz w innych nadzwyczajnych przypadkach, gdy byłoby to wskazane przykładowo w związku ze zmianami technologicznymi.
9. Plan ciągłości działania powinien zostać poddany testom badającym adekwatność i jego skuteczność w kontekście zapewnienia ciągłego i niezakłóconego prowadzenia działalności przez Zarządzającego posiadającego licencję, zarówno na etapie jego opracowania jak i w ramach

dokonywanych przeglądów. Testy powinny być oparte na każdorazowo przygotowywanych na ich potrzeby scenariuszach, które:

a. uwzględniają zagrożenia, na które Zarządzający posiadający licencję może być narażony w związku z wykonywaną działalnością oraz środki im zapobiegania;
b. są zaplanowane w taki sposób, aby sprawdzić założenia, na których opiera się plan ciągłości działania, w tym zasady zarządzania i plany komunikacji kryzysowej;
c. zapewniają możliwość udokumentowana ich realizacji.

10. W przypadku udziału w teście podmiotów zewnętrznych należy ograniczyć ich dostęp do scenariusza testu i informacji na temat przebiegu akcji awaryjnej do minimalnego poziomu niezbędnego do przeprowadzenia testu zgodnie z przyjętym scenariuszem.
11. Testowanie powinno również uwzględniać regulacje wewnętrzne Zarządzającego posiadającego licencję, na podstawie których możliwe będzie przeprowadzenie oceny, czy odpowiednie jednostki wewnętrzne Zarządzającego posiadającego licencję są w stanie odpowiednio reagować na sytuacje wymagające wdrożenia rozwiązań przewidzianych w planie ciągłości działania.


ZPF
Związek
Przedsiębiorstw
Finansowych
w Polsce